

Sahra Golghalyani

Der internationale Schutz der Privatsphäre vor geheimdienstlicher Überwachung

Die geheimdienstliche Ausspähung der Telekommunikation von Individuen im Lichte des IPpbR und der EMRK

Universitätsverlag Göttingen

Sahra Golghalyani

Der internationale Schutz der Privatsphäre vor geheimdienstlicher Überwachung



erschienen im Universitätsverlag Göttingen 2022

Sahra Golghalyani

Der internationale Schutz der Privatsphäre vor geheimdienstlicher Überwachung

Die geheimdienstliche Ausspähung der Telekommunikation von Individuen im Lichte des IPpbR und der EMRK

Universitätsverlag Göttingen
2022

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

Dissertation, Georg-August-Universität Göttingen



Satz und Layout: Sahra Golghalyani/Alice von Berg
Umschlaggestaltung: Hannah Böhlke/Margo Bargheer
Coverbild: Bild von https://aofirs.org/images/osint-keyboard.jpg

https://univerlag.uni-goettingen.de
ISBN: 978-3-86395-547-2
DOI: https://doi.org/10.17875/gup2022-2007

Danksagung

Diese Dissertation wurde im März 2020 bei der Juristischen Fakultät der Georg-August-Universität Göttingen eingereicht. Literatur und Rechtsprechung wurden bis Oktober 2021 eingearbeitet.

Mein besonderer Dank gilt Frau *Prof. Dr. Anja Seibert-Fohr*, die mir die Erstellung dieser Dissertation ermöglicht hat. Ihr danke ich auch für die lehrreiche Zeit, in der ich ihrer Tätigkeit im UN-Menschenrechtsausschuss assistieren durfte.

Zudem danke ich Herrn *Prof. Dr. Dr. h.c. Kai Ambos* für die Erstellung des Zweitgutachtens und die hilfreichen Anmerkungen.

Herrn *Robert Hennicke* danke ich vielmals für die gründliche und zügige Durchsicht der Arbeit.

Ohne die bedingungslose Unterstützung meiner Familie wäre diese Dissertation nie entstanden. Ihnen ist diese Arbeit gewidmet. Mein herzlichster Dank gilt meinen Eltern, *Simin Arfaee* und *Mahmoud Golghalyani*, die mich in jeder Lebensphase gefördert und ermutigt haben. Meinem Mann *Sadroddin Alavi Panah* verdanke ich, dass ich die Arbeit auch in schwierigen Zeiten fertig stellen konnte. Als Ehemann und als Vater unserer Tochter *Mahdis* war seine wertvolle Unterstützung immer präsent.

Berlin, im Dezember 2021 *Sahra Golghalyani*

Inhaltsverzeichnis

Abkürzungsverzeichnis

AfCRMV	Afrikanischen Charta der Rechte der Menschen und Völker
AMRK	Amerikanische Menschenrechtskonvention
BDSG	Bundesdatenschutzgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
Ebd.	Ebenda
EGMR	Europäischer Gerichtshof für Menschenrechte
EKMR	Europäische Kommission für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EUGH	Europäischer Gerichtshof

GCHQ	Government Communications Headquarters
Hervorh. d. Verf.	Hervorhebung durch den Verfasser
Hrsg.	Herausgeber
i.e.S	Im engeren Sinne
IGH	Internationaler Gerichtshof
ILC	International Law Commission
IPbpR	Internationaler Pekt über bürgerliche und politische Rechte
IPwskR	Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte
m.w.N.	Mit weiteren Nachweisen
MRA	UN-Menschenrechtsausschuss
NSA	National Security Agency
OHCHR	Hoher Kommissar der Vereinten Nationen für Menschenrechte
Rn.	Randnummer
Rs.	Rechtssache
UN-Charta	Charta der Vereinten Nationen
WVRK	Wiener Vertragsrechtskonvention

Einleitung

„Man konnte natürlich nie wissen, ob man im Augenblick gerade beobachtet wurde oder nicht. Wie oft oder nach welchem System sich die Gedankenpolizei in jede Privatleitung einschaltete, darüber ließ sich bloß spekulieren. Es war sogar denkbar, daß sie ständig alle beobachtete. Sie konnte sich jedenfalls jederzeit in jede Leitung einschalten. Man mußte folglich in der Annahme leben – und tat dies auch aus Gewohnheit, die einem zum Instinkt wurde –, daß jedes Geräusch, das man verursachte, gehört und, außer bei Dunkelheit, jede Bewegung beäugt wurde."

George Orwell, 1984[1]

George Orwells Darstellungen in seinem Roman „1984" wirkten zur Zeit der Veröffentlichung im Jahre 1948 wohl als irreale Fiktion eines ingeniösen Autors. Liest man Orwells Meisterwerk heute, 70 Jahre später, erscheint das beschriebene Bild des gläsernen Bürgers und die Allgegenwärtigkeit des Überwachungsstaates erschreckend realistisch. Die erstaunliche Dynamik in der technologischen Entwicklung hat in den vergangenen Jahrzehnten eine regelrechte digitale Revolution bewirkt.

---

[1] *Orwell*, 1984, S. 9.

Die moderne Informations- und Kommunikationstechnologie ermöglicht nicht nur die schnelle Massenabwicklung privater Korrespondenz, sondern eröffnet auch den Geheimdiensten die Tore für eine umfassende Telekommunikationsüberwachung. In Reaktion auf komplexe Sicherheitsherausforderungen der heutigen Welt, insbesondere auf den internationalen Terrorismus, hat die undifferenzierte Massenüberwachung privater Korrespondenzen inzwischen in zahlreichen Staaten Einzug in die geheimdienstlichen Überwachungssysteme gefunden. Der Zusammenprall von nationaler Sicherheit und dem Individualinteresse auf Privatsphärenschutz im Fall der geheimdienstlichen Überwachung stellt ein besonders augenfälliges Exempel der Kollision von Sicherheit und Freiheit dar. Inwieweit darf dabei ein Staat auf Kosten der individuellen Freiheit einen Raum der Sicherheit schaffen? Ausgangspunkt für die Beantwortung dieser grundlegenden Frage ist der Menschenrechtsschutz, der den Schutzumfang und die Schutzgrenzen individueller Grundfreiheiten definiert. So sind auch geheimdienstliche Überwachungssysteme zum Zweck der Staatssicherheit am Maß des Menschenrechtschutzes zu bewerten. Der Schutz der Privatsphäre ist ein menschliches Grundbedürfnis und als solches menschenrechtlich sowohl auf nationaler als auch auf internationaler Ebene kodifiziert.[2] Im Untersuchungsfokus der vorliegenden Arbeit steht in diesem Sinne die Frage danach, inwieweit die geheimdienstliche Überwachung privater Telekommunikation mit dem internationalen Menschenrecht auf Privatsphäre vereinbar ist.

Die Untersuchung widmet sich allein dem in internationalen Menschenrechtsverträgen verankerten Schutz der Privatsphäre. Denn im Bereich der geheimdienstlichen Überwachung ist die internationale Menschenrechtsebene vornehmlich aus zwei Gründen besonders bedeutsam. Einerseits gehen heute Überwachungsmaßnahmen häufig über Staatsgrenzen hinaus und betreffen auch Individuen auf fremden Hoheitsgebieten. Zum anderen ist davon auszugehen, dass die Staaten aus politischen und diplomatischen Gründen hinsichtlich der Ahndung von unrechtmäßigen transnationalen Überwachungsmaßnahmen eher zurückhaltend sind. Hier wird die enorme Bedeutung der unabhängigen internationalen Menschenrechtsspruchkörper deutlich, die auch in diesem politisch sensiblen Bereich unabhängig die Verletzung von internationalen Menschenrechtsverstößen feststellen. Dabei ist die vorliegende Arbeit auf das in Art. 17 IPbpR und in Art. 8 EMRK niedergelegte Menschenrecht auf Privatsphäre fokussiert. Der verbindliche IPbpR hat aufgrund seiner globalen Geltung universellen Charakter, dessen Umsetzung vom unabhängigen UN-Menschenrechtsausschuss überwacht wird. Hinsichtlich der EMRK liegt eine außergewöhnlich umfassende und weitgefächerte Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte vor. Die beiden Menschenrechtspakte

[2] In Deutschland ist das allgemeine Recht des Einzelnen auf Achtung und freie Entfaltung seiner Persönlichkeit etwa in Art. 2 Abs. 1 in Verbindung mit Art. 1 GG niedergelegt. Auf internationaler Ebene wird die Privatsphäre beispielsweise in Art. 17 IPbpR, Art. 8 EMRK oder Art. 11 AMRK geschützt.

stellen damit für die Beantwortung der zentralen Fragestellung ausgezeichnete Forschungsgrundlagen dar.

Die vorliegende Untersuchung befasst sich zudem allein mit den Spionagehandlungen *staatlicher* Geheimdienste. Der Fokus der Dissertation liegt auf dem konkreten Akt der geheimdienstlichen Informationsbeschaffung. Gegenstand der Untersuchung ist dabei die Telekommunikationsüberwachung als eine gewichtige Form der geheimdienstlichen Methoden zur Gewinnung von Informationen. Die konkreten Arbeitsweisen im Bereich der Telekommunikationsüberwachung sind freilich geheim und für die Allgemeinheit nicht zugänglich, sodass eine umfassende Beleuchtung aller geheimdienstlicher Operationsmodalitäten von vornherein ausgeschlossen ist. Dieser Umstand begrenzt zwar wissenschaftliche Analysen auf diesem Feld, schließt diese jedoch nicht aus. Denn trotz dieses Spezifikums der geheimdienstlichen Arbeit sind durchaus bestimmte Fakten über die Überwachungstechniken der Geheimdienste bekannt. So werden zuweilen etwa Informationspreisgaben durch die Geheimdienste selbst bewusst gesteuert oder aber Insider und *Whistleblower* tragen sensible interne Informationen über die geheimdienstliche Arbeit heraus. Die gemeinhin bekannten „*Snowden*-Enthüllungen“[3] sind ein Beispiel für dieses Phänomen. Auch wenn diese Informationen nur einzelne Fragmente darstellen, so geben die bisher bekannten Fakten zumindest ein ausreichend definiertes Bild über die heutigen Methoden der Telekommunikationsausspähung wieder, um diese für politische und insbesondere für wissenschaftliche Analysen zugänglich zu machen. Auf Grundlage dieser Informationen ergeben sich in Abhängigkeit der konkreten Art der Überwachungstechnik, des Ortes der Überwachungsdurchführung und des Aufenthaltsortes des Individuums vielfältige Überwachungskonstellationen. Vor diesem Hintergrund kann die vorliegende Dissertation nicht den Anspruch erheben, die geheimdienstliche Telekommunikationsausspähung erschöpfend und in jeglicher Ausprägung zu ergründen. Die vorliegende Untersuchung unternimmt vielmehr den Versuch, in Orientierung an den bekannten Fakten realitätsnahe Überwachungskonstellationen zu bilden, diese zu systematisieren und einer menschenrechtlichen Überprüfung zu unterziehen.

Da der Überwachungsradius der modernen Geheimdienste über die Grenzen ihres Staatsgebiets hinausgeht, stellt sich im Rahmen dieser menschenrechtlichen Überprüfung das besondere Problem der extraterritorialen Jurisdiktionsausübung der überwachenden Staaten. Die in der bisherigen Spruchpraxis des MRA und des EGMR entwickelten Kriterien zur Begründung der extraterritorialen Jurisdiktionsausübung erfassen das Phänomen der grenzüberschreitenden Telekommuni-

[3] *Edward Snowden* ist ein IT-Spezialist und ehemaliger Geheimdienstmitarbeiter des US-Geheimdienstes NSA. Im Jahr 2013 veröffentlichte er streng geheime Informationen über die umfassenden Überwachungspraktiken der NSA und des GCHQ. Zu den Enthüllungen siehe *Greenwald, Glenn and McAskill, Ewen* „NSA Prism Program Taps in to User Data of Apple, Google and Others“ The Guardian 7. Juni 2013, abrufbar unter http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link [zuletzt abgerufen 22.02.2020].

kationsüberwachung nicht. Im Rahmen der vorliegenden Arbeit wird ein Konzept entworfen, das in Weiterentwicklung der bisherigen Judikatur die Grundlagen, Voraussetzungen und Rechtsfolgen der extraterritorialen Jurisdiktionsausübung in Fällen der grenzüberschreitenden Telekommunikationsüberwachung darlegt.

Die Arbeit ist in drei Abschnitte untergliedert. Im 1. Abschnitt werden die Grundlagen des Forschungsgegenstandes dargestellt. Einerseits werden dabei die Begriffsumrisse und die digitale Dimension der Privatsphäre in der heutigen Zeit sowie andererseits die Grundzüge der geheimdienstlichen Überwachung im 21. Jahrhundert aufgezeigt. Im 2. Abschnitt wird sodann die innerstaatliche Telekommunikationsüberwachung menschenrechtlich untersucht. Nach einer einführenden Darstellung des internationalen Schutzes der Privatsphäre im IPbpR und in der EMRK wird anschließend die zentrale Frage nach der Vereinbarkeit der geheimdienstlichen Ausspähung der Telekommunikation mit dem menschenrechtlichen Schutz auf Privatsphäre beleuchtet. Dabei wird insbesondere die einschlägige Judikatur des MRA und des EGMR zu den aus Art. 17 IPbpR und Art. 8 EMRK hervorgehenden Voraussetzungen herausgearbeitet, um die Menschenrechtskonformität der modernen Telekommunikations-überwachung an diesen Kriterien zu messen. Schließlich wird im 3. Abschnitt der Fokus auf die grenzüberschreitende Telekommunikationsüberwachung gerichtet. Hierbei wird untersucht, inwieweit eine Verletzung des Menschenrechts auf Privatsphäre durch den überwachenden Drittstaat, aber auch durch den Aufenthaltsstaat des betroffenen Individuums in Betracht kommt. In diesem Zusammenhang werden insbesondere Fragen zur extraterritorialen Anwendbarkeit der Menschenrechtspakte sowie zur Schutzpflichtverletzung durch den Aufenthaltsstaat beantwortet. Des Weiteren wird abschließend die Menschenrechtskonformität von *Intelligence Sharing* untersucht.

1. Abschnitt: Grundlagen

A. Privatsphäre im 21. Jahrhundert

Der Titel dieses Kapitels suggeriert, dass sich die „Privatsphäre" im 21. Jahrhundert von der „Privatsphäre" in den Jahrhunderten zuvor unterscheidet. Dabei ist der Schutz der Privatsphäre ein natürliches menschliches Urbedürfnis, das seit jeher einen empfindlichen Wert in der persönlichen Lebensführung eines Individuums darstellt.[4] Der Begriff „Privatsphäre" unterliegt jedoch einer Dynamik, die dem gesellschaftlich-historischen Wandel folgt.[5] Die konkrete Grenzziehung zwischen Privatheit und Öffentlichkeit wird durch das kulturelle und soziale Umfeld eines Individuums beeinflusst.[6] Insbesondere die rasante Entwicklung der Kommunikations- und Informationstechnologie im 21. Jahrhundert hat die Definition der Privatsphäre weltweit kennzeichnend beeinflusst. Die individuelle „Privatsphäre" hat im 21. Jahrhundert durchaus neue Konturen gewonnen, ist aber andererseits auch größeren Gefahren ausgesetzt. Nach einer allgemeinen Begriffsbestimmung von

---

[4] Erste philosophische Unterscheidungen zwischen dem Privaten und der Öffentlichkeit gehen bis in die Antike zurück; zur ausführlichen Geschichte der „Privatsphäre" vgl. *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 23 ff. m.w.N.

[5] Ebd., S. 23.

[6] Ebd., S. 55.

„Privatsphäre", „Daten" und „Metadaten" wird im Folgenden anschließend anhand von Statistiken dargelegt, wie die moderne Informationstechnologie die Konturen der Privatsphäre geprägt hat.

I. Begriffsbestimmung: „Privatsphäre", „Daten" und „Metadaten"

Im Kern beschreibt der abstrakte und weite Begriff „Privatsphäre" einen persönlichen Bereich, in dem das Individuum freie und ungestörte Gestaltungsfreiheit und Autonomie über sein privates Leben genießt.[7] Hinsichtlich der inhaltlichen Konturen des abstrakten Begriffs der „Privatsphäre" gibt es jedoch keine allgemein anerkannte Definition. Es gibt zahlreiche Definitionsansätze, die in Abhängigkeit des zeitlichen, örtlichen und kulturellen Kontextes enger oder weiter sind und unterschiedliche Aspekte umfassen.[8] Im Bereich des Menschenrechtsschutzes werden die Grenzen des menschenrechtlichen Schutzbereiches der „Privatsphäre" in den einzelnen Menschenrechtsverträgen definiert. In dieser Dissertation wird der im IPbpR und in der EMRK niedergelegte Schutz der Privatsphäre im 2. Abschnitt näher erläutert.[9]

Unter „Daten" sind im IT-spezifischen Sinne jede Form von alphanumerischen Zeichen zu verstehen, die auf Datenträgern festgehalten werden.[10] Die Bedeutung dieser Zeichen ist isoliert betrachtet häufig nicht zu erschließen. Erst in einem spezifischen Kontext und in Kombination mit weiteren Angaben wird die Bedeutung der Daten erkennbar. Die reinen Daten sind damit Grundlage von Informationen.[11] So kann beispielsweise die Bedeutung einer beliebig erscheinenden Ziffernabfolge erst erschlossen werden, wenn sie mit den Begriffen „Kundennummer der Person X" angegeben wird. Die Zahlenabfolge wäre in diesem Beispiel das Datum, das erst im Zusammenhang mit den genannten Begriffen zu einer sinnhaften Information über die Kundennummer einer Person wird. Im nationalen und internationalen Rechtsraum ist indes der Begriff „personenbezogene" Daten sehr bedeutsam. Damit sind grundsätzlich Daten gemeint, die sich auf eine bestimmte oder bestimmbare Person beziehen.[12] Die konkreten Umrisse dieser Begrifflichkeit werden im Rahmen der Untersuchung der einzelnen Rechtsregime dargestellt.

„Metadaten"[13] sind im Bereich der Telekommunikations- und Internetdienstleistungen wiederum die Daten, die im Rahmen der Datenübermittlung unvermeid-

---

[7] Vgl. auch Office of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age: Report of the OHCHR, A/HRC/39/29, 03. August 2018, Rn. 5.

[8] Eine Zusammenstellung über bekannte Theorien zum Begriff der „Privatsphäre" ist im Werk von *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 8 ff. zu finden.

[9] Siehe unten 2. Abschnitt, Unterabschnitte A. I und A. II.

[10] *Schmidl,* IT-Recht von A-Z, S. 66.

[11] *Ronellenfitsch* in Wolff/Brink, Datenschutzrecht in Bund und Ländern, Kommentar, S. 375.

[12] *Eßer* in Eßer/Kramer/von Lewinski, DSGVO/BDSG Kommentar, S. 72, Rn. 6.

[13] Üblich sind auch die bedeutungsgleichen Begriffe „Verkehrsdaten" oder „Verbindungsdaten". Im deutschen Telekommunikationsgesetz wird etwa der Begriff „Verkehrsdaten" verwendet (§ 96 TKG).

bar generiert werden. Jegliche Daten, die hinsichtlich der Erbringung der Dienstleistung üblicherweise anfallen und von den Dienstleistern erhoben und verarbeitet werden, sind „Metadaten".[14] Dazu gehören beispielsweise die Rufnummer oder andere Benutzerkennungen (wie etwa IP-Adressen) sowie Datum, Uhrzeit und Dauer der in Anspruch genommenen Dienstleistung.[15] Auch die Standorte von mobilen Geräten sowie die übermittelten Datenmengen können als Metadaten im Rahmen der jeweiligen Telekommunikationsverbindung anfallen.[16] Die Metadaten betreffen folglich nicht den Inhalt der Telekommunikation.

II. „Privatsphäre" in der digitalisierten Welt

Moderne Informations- und Kommunikationstechnologie ist heute in den allermeisten privaten Haushalten üblicher Bestandteil der Haushaltsausstattung. Zahlen des Statistischen Bundesamtes belegen, dass 2017 etwa 90% der deutschen Privathaushalte über einen PC verfügten. Auch Mobiltelefone sind heute nicht nur in Deutschland in über 95% der Haushalte vorhanden.[17] Statistiken der Weltbank zeigen, dass in den meisten Nationen ein überwiegender Anteil der Personen über Mobilfunkanschlüsse verfügt. In einigen Ländern sind im Jahr 2014 auf 100 Personen sogar über 200 Mobilfunkanschlüsse registriert worden.[18]

In diesem Zusammenhang sind indes nicht nur die aufgezeigten hohen Prozentsätze als solche augenfällig, sondern auch die rasante Dynamik dieser Entwicklung ist besonders interessant. So verfügte im Jahr 1990 nur eine verschwindend kleine Anzahl von Personen in einigen wohlhabenden Ländern über einen Mobilfunkanschluss.[19] Während beispielsweise in Japan 1990 nur ein Mobilfunkanschluss auf 100 Personen fiel, waren es 2015 – 25 Jahre später – bereits 120 Mobilfunk-

[14] So wird etwa der Begriff „Verkehrsdaten" in § 3 Nr. 30 TKG definiert. Vgl. auch *Keller,* Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit, S. 21 f.

[15] Vgl. auch *Keller/Braun/Hoppe,* Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, S. 23 f.

[16] *Paefgen,* Persönlichkeitsrechte im Internet, S. 23 f. Vgl. außerdem § 96 TKG.

[17] Statistisches Bundesamt (Hrsg.): Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik im Zeitvergleich (Deutschland), abrufbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Ausstattung-Gebrauchsgueter/Tabellen/liste-infotechnik-d.html;jsessionid=2965DA9FFC96086A98FFDF739AD1641C.internet721 [zuletzt abgerufen: 01.12.2021].

[18] The World Bank (Hrsg.): Mobile cellular subscriptions (per 100 people), abrufbar unter: http://data.worldbank.org/indicator/IT.CEL.SETS.P2/countries [zuletzt abgerufen: 01.12.2021], in den Vereinigten Arabischen Emiraten waren im Jahr 2017 auf 100 Personen etwa 210 Mobilfunkanschlüsse vorhanden.

[19] Ebd.

anschlüsse.[20] Binnen 25 Jahren hat somit die moderne Kommunikationstechnologie Einzug in das alltägliche Leben vieler Menschen gefunden.[21]

Dieselbe Entwicklung ist hinsichtlich der globalen Internetnutzung zu beobachten. In der ersten Hälfte der neunziger Jahre begann allmählich die private Nutzung des Internets in einigen wirtschaftsstarken Ländern. Seitdem hat die private Nutzung des Internets stetig zugenommen.[22] Heute wird das Internet in zahlreichen Haushalten regelmäßig genutzt,[23] wobei die Unterschiede zwischen einzelnen Ländern erheblich sind. In Deutschland wurde in den ersten Monaten des Jahres 2018 das Internet in 89% der privaten Haushalte fast täglich genutzt.[24] In Entwicklungsländern wie Eritrea oder Myanmar ist die Internetnutzung innerhalb der Bevölkerung hingegen auch heute noch gering.[25] Trotz allem geht aus den Statistiken der Weltbank die globale Zunahme der Internetnutzung unzweifelhaft hervor. Durch Smartphones ist der Zugang zum Internet heute sogar von fast jedem Ort und zu jeder Zeit möglich.

Das Internet ist ein unerschöpflicher Ozean aus Informationen und virtuellen Dienstleistungen, die sich über alle denkbaren Lebensbereiche und Branchen erstreckt. Ob für private oder professionelle Zwecke – das Internet stellt heute in vielen Gesellschaften ein allgegenwärtiges und alltägliches Medium für Informationsaustausch und Kommunikation dar. Selbst staatliche Institutionen nutzen heute in vielen Bereichen das Internet, so etwa zur Abwicklung und Verarbeitung von Verwaltungsaufgaben. Zeitintensive Behördengänge werden durch sekundenschnelle Online-Datenverarbeitung ersetzt, wodurch indes nicht nur die antragstellenden Privatpersonen ihre Anträge deutlich schneller in den Verwaltungsapparat einreichen können, sondern insbesondere die Verwaltung selbst erheblich entlastet

---

[20] Die Statistik der Weltbank (Fn. 18) belegt, dass diese Entwicklung in vielen Ländern zu beobachten ist.

[21] Siehe auch *Moser-Knierim,* Vorratsdatenspeicherung, S. 18 f., die in diesem Zusammenhang die Bezeichnung „Digitale Revolution“ verwendet.

[22] The World Bank (Hrsg.): Individuals using the Internet (% of population), abrufbar unter: https://data.worldbank.org/indicator/IT.NET.USER.ZS, http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default[zuletzt abgerufen: 01.12.2021].

[23] Ebd. Danach haben 2014 in 44 Staaten zwischen 60 und 80 Personen (von insgesamt 100 Personen) das Internet genutzt (Beispiele: Azerbaijan 61,0%, Chile 72,4%, Tschechien 79.7%) und in 30 Staaten waren es über 80 Personen (Beispiele: Neuseeland 85,5%, Schweden 92,5%, Dänemark 96%).

[24] Statistisches Bundesamt (Hrsg.): Wirtschaftsrechnungen – Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien, Fachserie 15, Reihe 4, Wiesbaden 2018, S. 15, abrufbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/_inhalt.html#sprg234968 [zuletzt abgerufen: 01.12.2021].

[25] The World Bank (Hrsg.): Individuals using the Internet (% of population), abrufbar unter: https://data.worldbank.org/indicator/IT.NET.USER.ZS [zuletzt abgerufen: 01.12.2021].

wird.[26] *Social-Media*, wie etwa *Facebook*, *Instagram* oder *Twitter*, bieten eine Plattform für soziale Vernetzung und Kommunikation, die heute von allen Generationen gerne genutzt wird. Nach Umfragen des *Pew Research Center* nutzten 2015 72% der befragten US-amerikanischen Internetnutzer *Facebook*. Hiervon gaben wiederum 70% an, *Facebook* täglich zu nutzen.[27]

Die vielfältigen Facetten des Internets erleichtern und erweitern unfraglich den Alltag ganzer Gesellschaften. Allerdings ist die Nutzung des Internets mit der Preisgabe von persönlichen Informationen und Daten verbunden.[28] Jede Inanspruchnahme von Online-Diensten hinterlässt digitale Spuren. So ist die Veröffentlichung privater Fotos oder die Bekanntgabe des aktuellen Aufenthaltsorts eines Individuums auf *Facebook* unzweifelhaft eine bewusste Entscheidung zur Preisgabe von Informationen. Auch bei Online-Einkäufen werden freiwillig Informationen über Identität, Anschrift und sogar Bankverbindung angegeben. In diesen Fällen geben die Nutzer zum Zweck der Nutzung von Online-Dienstleistungen persönliche Informationen weiter. Doch ist vielen Nutzern häufig gar nicht bewusst, dass die Nutzung vieler Online-Dienste mit der Preisgabe von Daten verbunden ist. Gibt jemand beispielsweise einen Suchbegriff in die gängige Suchmaschine *Google* ein, so werden sowohl die IP-Adresse des Nutzers als auch die eingegebenen Suchbegriffe gespeichert.[29]

Die breite Nutzung der modernen Kommunikations- und Informationstechnologie belegt eindeutig, dass Privatsphäre heute auch eine digitale Dimension hat. Während sich in früheren Jahrhunderten Kernelemente des Privaten in den eigenen vier Wänden im Kreis der Familie befanden, sind im modernen Zeitalter jegliche Informationen in einem globalen Netzwerk unterwegs. Intimste Informationen befinden sich oftmals gar nicht mehr im Macht- und Zugriffsbereich der Betroffenen, sondern befinden sich etwa auf Servern von *Service Providern*. Der Schutz der Privatsphäre vor unbefugten und unerwünschten Einblicken steht im 21. Jahrhundert somit vor großen Herausforderungen. Infolge dieses einschneidenden technologischen Wandels der vergangenen Jahrzehnte, der viele Lebensbereiche unzähliger

[26] Ein Beispiel wäre die in Deutschland inzwischen etablierte elektronische Steuererklärung über die vom Finanzamt eingerichtete Plattform „ELSTER". Jegliche steuerlichen Anträge können von Privatpersonen, Arbeitgebern oder steuerberatenden Berufen online über diese Plattform nicht nur eingereicht werden, sondern auch die nachfolgende Kommunikation mit den zuständigen Finanzämtern in Deutschland erfolgt über „ELSTER". Siehe dazu die Homepage https://www.elster.de/e-portal/start [zuletzt abgerufen 01.12.2021].

[27] *Duggan, Maeve*: Mobile Messaging and Social Media – 2015, Pew Research Center (Hrsg.), August 2015, S. 10, abrufbar unter: https://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/ [zuletzt abgerufen: 01.12.2021] – Etwa 82% der befragten US-amerikanischen Internetnutzer zwischen 18 und 29 Jahren nutzen Facebook.

[28] *Bygrave*, Data Privacy Law, S. 5.

[29] Täglich werden über 3,5 Milliarden Suchen über Google durchgeführt, siehe dazu *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 51; vgl. auch Internet Live Stats, Google Search Statistics, URL: http://www.internetlivestats.com/google-search-statistics/ [01.12.2021]. Hier kann in Echtzeit die Anzahl der Google-Suchen im Laufe eines Tages verfolgt werden.

Individuen betrifft, ist der Datenschutz als eine Ausprägung des Schutzes der Privatsphäre immer mehr in den Vordergrund gerückt. Datenschutzbestimmungen haben sowohl auf nationaler als auch auf internationaler Ebene Einzug in die Rechtsordnungen gefunden.[30]

B. Geheimdienstliche Überwachung im 21. Jahrhundert

I. Begriffsbestimmung: „Geheimdienst“ und „*intelligence*“

Für einen historisch und politisch geprägten Begriff wie „Geheimdienst“ ist eine begriffliche Definition und Abgrenzung im Rahmen der vorliegenden Dissertation unabdingbar. Nachfolgend wird in diesem Sinne zunächst der deutsche Begriff „Geheimdienst“ definiert und im Anschluss untersucht, inwieweit dieser deutsche Begriff mit der englischsprachigen Bezeichnung „*intelligence*“ inhaltlich übereinstimmt. Die von beiden Bezeichnungen umfassten Begriffselemente werden aufgeschlüsselt, um diese letztlich für den Zweck dieser Untersuchung zu operationalisieren.

Ein Geheimdienst[31] ist eine staatliche Organisation zur Beschaffung, Bewertung und Interpretation vorwiegend geheimer Informationen militärischer, politischer, wirtschaftlicher und wissenschaftlicher Natur aus anderen Ländern, zum Zweck der Spionage sowie zur Spionageabwehr. Diese Definition ist angelehnt an die im Duden vorzufindende Begriffserklärung[32] und entspricht dabei den im Kerngehalt vergleichbaren Begriffsbestimmungen in Enzyklopädien und in der Fachliteratur.[33] Diese Definition wird der vorliegenden Dissertation zugrunde gelegt. Das Adjektiv „staatlich“ verdeutlicht dabei, dass das Untersuchungsspektrum dieser Dissertation auf staatliche Geheimdienste begrenzt ist. Andere Akteure im Bereich der Spionage – wie etwa rein private Überwachungsinstrumente – sind nicht Gegenstand der Untersuchung.

Vor dem Hintergrund, dass der wissenschaftliche Diskurs zum Themengebiet der Geheimdienste und der Spionage bisher überwiegend im angelsächsischen Raum stattfindet und demzufolge die relevante Literatur primär englischsprachig ist, kann der englische Begriff „*intelligence*“ an dieser Stelle nicht unberücksichtigt bleiben. Die hiesige Untersuchung basiert indes auf der These, dass der dargestellte

[30] Zum Datenschutz im IPbpR und in der EMRK siehe unten, 2. Abschnitt, Unterabschnitte A. I. 1. sowie 2.d. und A. II. 1. sowie 2. c.

[31] Davon ausgehend, dass die Begriffe „Geheimdienst“ und „Nachrichtendienst“ Synonyme darstellen, wird zum Zwecke der Einheitlichkeit in dieser Dissertation einzig der Begriff „Geheimdienst“ verwendet. Zur Synonymie der beiden Begriffe: *Roewer/Schäfer/Uhl,* Lexikon der Geheimdienste im 20. Jahrhundert, S. 160.

[32] Siehe https://www.duden.de/rechtschreibung/Geheimdienst [zuletzt abgerufen 01.12.2021].

[33] *Beck,* Sachwörterbuch der Politik, S. 326; *Roewer/Schäfer/Uhl,* Lexikon der Geheimdienste im 20. Jahrhundert, S. 160 und 310; *Meier, Hannemann/Meyer zum Felde,* Wörterbuch zur Sicherheitspolitik, S. 183; *Drechsler,* Gesellschaft und Staat. Lexikon der Politik, S. 390.

deutschsprachige Geheimdienstbegriff – d.h. die dargelegte Definition – mit der im englischsprachigen Raum üblichen Bezeichnung „*intelligence*" kongruent ist.

So wird die Bezeichnung „*intelligence*" zwar in der relevanten englischsprachigen Literatur intensiv diskutiert,[34] allerdings ist hinsichtlich der Grundpfeiler der Begrifflichkeit durchaus Einstimmigkeit erkennbar. Einigkeit besteht insbesondere darüber, dass „*intelligence*" ein weiter Begriff ist und einen entsprechend weiten Bedeutungsradius hat. „*Intelligence*" im institutionellen Sinne beschreibt die staatliche Institution, die zur Planung und Durchführung von Maßnahmen zur Informationsgewinnung im Interesse der staatlichen Entscheidungsträger beauftragt ist.[35] Des Weiteren umfasst der Begriff „*intelligence*" den Prozess der Informationsgewinnung und -analyse selbst.[36] „*Intelligence*" im materiellen Sinne ist schließlich das Ergebnis dieses Prozesses, also die gewonnene Information.[37]

Betrachtet man vor diesem Hintergrund erneut die deutsche Definition, wonach ein „Geheimdienst" eine staatliche Organisation zur Beschaffung vorwiegend geheimer Informationen ist, so ist die soeben dargestellte Untergliederung des englischen „*Intelligence*"-Begriffs wiederzuerkennen. So steht das Wort *Organisation* für den Geheimdienstbegriff im institutionellen Sinne; das wäre in Deutschland etwa der Bundesnachrichtendienst.[38] Die folgenden Begriffe *Beschaffung, Bewertung und Interpretation* umfassen indes den prozessualen Begriffssinn. So beschreibt *Beschaffung* als Oberbegriff letztlich die gesamte Abfolge der Informationsbeschaffung, einschließlich aller Handlungs- und Operationsmethoden. *Bewertung* und *Interpretation* betreffen wiederum die nachfolgenden Arbeitsprozesse. Schließlich impliziert die Definition auch eine materielle Dimension, indem als Beschaffungsergebnis *geheime Informationen militärischer, politischer, wirtschaftlicher und wissenschaftlicher Natur* benannt werden.

Somit kann an dieser Stelle festgehalten werden, dass sowohl der englische Begriff „*intelligence*" als auch der deutschsprachige Ausdruck „Geheimdienst" – wie er für diese Untersuchung definiert wird – jeweils die dargelegten institutionellen, prozessualen und materiellen Definitionsmerkmale umfassen.

---

[34] Wissenschaftliche Diskussionen zum Themengebiet der Geheimdienste finden überwiegend im angelsächsischen Raum statt, sodass auch Fragen der Terminologie bisher fast ausschließlich den englischsprachigen Ausdruck „*intelligence*" betreffen. Abgesehen von historischen Untersuchungen, hat sich in Deutschland indes noch kein breiter wissenschaftlicher Diskurs zum Thema Geheimdienste etabliert; siehe dazu etwa *Blancke,* Geheimdienste und globalisierte Risiken, S. 10.

[35] Siehe etwa *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S.7 ff., der „*intelligence*" im institutionellen Sinne am Beispiel der USA erläutert.

[36] Ebd., S.12 ff.

[37] Ebd., S. 21 ff.

[38] Siehe die offizielle Webseite des BND: https://www.bnd.bund.de/DE/Startseite/startseite_node.html [zuletzt abgerufen 01.12.2021].

II. Die Funktion geheimdienstlicher Überwachung im Kontext historischer und gegenwärtiger sicherheitspolitischer Herausforderungen

Die dargelegte Definition kennzeichnet zwar die begrifflichen Konturen eines Geheimdienstes und besagt zudem, dass die Informationsbeschaffung zum Zwecke der Spionage und zur Spionageabwehr erfolgt. Dabei bleibt aber offen, warum die Staaten durch ihre Geheimdienste überhaupt Spionage und auf der anderen Seite reaktiv die Abwehr solcher Akte vornehmen. Welche Funktion erfüllt die Praxis geheimdienstlicher Überwachung? Und inwieweit hat sich der Zweck der geheimdienstlichen Überwachung angesichts der auffallend langen Historie dieser Praxis im Laufe der Jahrhunderte und gar Jahrtausende gewandelt?

Grundsätzliches Ziel der geheimdienstlichen Überwachung ist im Allgemeinen – historisch und politisch übergreifend – zunächst das Beschaffen und Bereitstellen von Informationen über potenzielle Risiken[39], die die Interessen eines Staates tangieren können.[40]

Geheimdienste beschaffen durch spezifische Spionagemethoden entscheidungsrelevante Informationen und stellen diese den politischen Entscheidungsträgern des Staates zur Verfügung. Auf Grundlage der hierdurch erzielten Informationshoheit sollen staatliche Entscheidungsträger potenzielle Gefahren identifizieren können,[41] um auf Grundlage dieser Risikoeinschätzung gezielte politische Entscheidungen über strategische Maßnahmen zum Schutz der nationalen Interessen sowie zur Abwehr der Gefahren treffen zu können.[42]

Diese allgemeine Funktion ist im Laufe der Geschichte – von der Antike bis heute – im Kern unverändert geblieben. Zweck der Spionage war schon immer und ist noch heute die Informationsbeschaffung zum Schutz nationaler Interessen. Ein signifikanter Wandel ist indes hinsichtlich der Art der Risiken, die die Staatsinteressen potenziell gefährden können, zu beobachten. Dabei ist in diesem Zusammenhang vorweg anzumerken, dass der Begriff der Staatsinteressen sicherlich sehr weit ist. Die Definition und Konkretisierung der Interessen ist Sache der Nationalstaaten. Primäres Interesse eines Staates ist unzweifelhaft – sowohl heute wie auch in der Vergangenheit – die nationale Sicherheit.[43] Dies umfasst sowohl die Sicherung der nationalen Grenzen und letztlich den territorialen und politischen Bestand des Staates, aber gewiss auch den Schutz der eigenen Staatsbürger.

So strebten auch die antiken Herrscher nach der Aufrechterhaltung und darüber hinaus nach der territorialen Expansion ihrer Großreiche. Hierzu setzten sie Mittel

---

[39] Zum politischen Risikobegriff siehe, *Daase*, Internationale Risikopolitik, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 11 ff.
[40] *Gill/Phythian,* Intelligence in an Insecure World, S. 29; *Shulsky/Schmitt,* Silent Warfare, S. 1.
[41] *Blancke*, Geheimdienste und Globalisierte Risiken, S. 37.
[42] *Johnson*, Secret Agencies, S. 2–3; *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 5; *Lowenthal,* Intelligence. From Secrets to Policy, S. 2–3.
[43] *Shulsky/Schmitt,* Silent Warfare, S. 3.

der Spionage ein, um Informationen über äußere und innere Gefahren zu erhalten, die diesem Interesse entgegenstanden. Die Gefahrenquellen waren indes nicht unbekannt. Da die Herrschaft in diesen Großreichen auf ein religiös und kulturell begründetes Fundament ruhte, sorgte insbesondere die Loyalität der religiös einheitlichen Bevölkerung für die innere Stabilität.[44] Die Eroberung neuer Territorien samt neuen Bevölkerungsgruppen konnte indes eine Gefahr für die umfassende Loyalität bedeuten und letztlich die hierauf beruhende Stabilität erschüttern.[45] Fremde Völker mussten integriert und mögliche Aufstände niedergeschlagen werden. Zudem musste sichergestellt werden, dass innerhalb des Reiches – insbesondere in den neuen Territorien – keine unabhängige Parallelherrschaft entsteht; diese hätte anderenfalls die regierende Universalherrschaft untergraben.[46] Insbesondere aber stellten aufstrebende Reiche, die ebenfalls ihr Territorium ausweiten und bestehende Großreiche erobern wollten, eine ernsthafte Gefahr dar. Sicherlich waren den antiken Herrschern die konkrete Art sowie der Zeitpunkt des Eintritts der Gefährdung, etwa ein vom Gegner strategisch organisierter Feldzug, nicht von vornherein bekannt. Eben zur Auskundschaftung solcher Informationen wurden Spione eingesetzt. Allerdings kannten die Herrscher ihre Gegner, sodass eine Lokalisierung der Gefahrenquelle durchaus möglich war. Sie wussten – auch aufgrund der Spionage –, welche Reiche aufstrebten und wer ihnen gegenüber feindlich gesinnt war. Die Feinde – ob innerhalb oder außerhalb des Reiches – waren mithin bekannt.

Erst im Fortgang der Geschichte wurden die zwischenstaatlichen Verhältnisse und letztlich auch die Risikoeinschätzung allmählich komplexer. Die ersten amtlichen Geheimdienste, die als staatliche Behörden agierten, entstanden zu Beginn des 20. Jahrhunderts.[47] Während des kalten Krieges, in der die Geheimdienste „eine Bedeutung wie nie zuvor in der modernen Staatengeschichte“[48] gewannen, standen sich nicht mehr einzelne, isolierte Staaten gegenüber. Es herrschte vielmehr eine Konfrontation zwischen dem Ostblock und dem Westen, d.h. auf beiden Seiten waren mehrere Staaten involviert. Darüber hinaus herrschte zudem eine Konfrontation zwischen zwei Staatenbündnissen, nämlich der NATO und dem Warschauer Pakt. Trotz dieser unverkennbaren Zunahme an Verflechtung und Komplexität, die ein historisches Resultat der politischen Entwicklungen in den Jahrhunderten zuvor war, herrschte eine stabile Gefährdungslage und eine klare Bipolarität.[49] So waren zwar zahlreiche Nationen in diesem Konflikt verstrickt, dennoch waren die Akteure als solche weiterhin identifizierbar.[50] Die Staaten waren letztlich weiterhin die

[44] *Krieger*, Geschichte der Geheimdienste, S. 20.
[45] Ebd.
[46] Ebd.
[47] *Knightley,* Die Geschichte der Spionage im 20. Jahrhundert, S. 8.
[48] *Krieger*, Geschichte der Geheimdienste, S. 251.
[49] *Daase*, Internationale Risikopolitik, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 7 und 9; *Dearlove,* National Security and Public Anxiety, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence, S. 33.
[50] Ebd.

zentralen Gefahrenquellen.[51] Das Ziel der geheimdienstlichen Überwachung war eindeutig: Das militärische Potenzial sowie die strategischen Pläne des Gegners sollten weitgehend in Erfahrung gebracht werden.[52]

Die beschriebene Klarheit der Gefährdungslage sowie die Identifizierbarkeit der agierenden Akteure während des kalten Krieges leuchtet umso mehr ein, wenn man die Situation nach 1990, vor allem aber nach der Jahrtausendwende näher betrachtet. Denn nunmehr waren in erster Linie nicht mehr bestimmte Staaten Gefährdungsquellen. Seit dem Ende des Kalten Krieges, im Zeitalter der Globalisierung, sind die Staaten mit neuen sicherheitspolitischen Herausforderungen konfrontiert, die gerade nicht von einzelnen Staaten ausgehen, wie etwa Terrorismus, Klimawandel, Migration oder Finanzstabilität.[53] Während im kalten Krieg die Spionage der Auskundschaftung von Informationen etwa über das militärische Potenzial[54] oder über geplante Aktionen des bekannten Gegners diente, geht die geheimdienstliche Überwachung nun angesichts dieser neuen Risikolage einen nicht unwesentlichen Schritt weiter. So muss nun auch die Quelle der Gefahr, d.h. der zentrale Akteur, zunächst identifiziert werden. Ehemals beantworteten die Geheimdienste insbesondere die Frage „Was plant der Gegner?“, während heute gefragt wird „Wer ist der Gegner?“.

Heute steht der internationale Terrorismus unzweifelhaft im Fokus der nationalen Sicherheitspolitik. Dabei ist Terrorismus im weiteren Sinne kein modernes Phänomen. Vorläufer des heutigen Terrorismus reichen bis in die Antike zurück und haben insbesondere seit dem 19. Jahrhundert in der Weltgeschichte eine zunehmende Rolle gespielt.[55] Allerdings haben sich die Motive und Strukturen des Terrorismus im Laufe der Zeit stetig geändert.[56] Während die früheren Formen des Terrorismus primär innerstaatlich orientiert waren, ist der transnationale grenzüberschreitende Terrorismus ein modernes Phänomen, das sich als Schattenseite der Globalisierung herausgestellt hat.[57] Der heutige internationale Terrorismus wird zumeist von nicht-staatlichen Akteuren getragen, die oftmals unabhängig von Nationalstaaten agieren.[58] Die Terrornetzwerke dieser Akteure sind global organisiert. Diese Dezentralisierung ist ein wesentliches Merkmal des modernen Terrorismus.[59]

---

[51] *Hagmann*, (In-)Security and the Production of International Relations, S. 186.
[52] *Blancke*, Geheimdienste und Globalisierte Risiken, S. 2.
[53] *Hagmann*, (In-)Security and the Production of International Relations, S. 186.
[54] *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 15.
[55] *Ramakrishna*, From ‚Old‘ to ‚New‘ Terrorism, in Gill (Hrsg.), Handbook of Security, S. 160.
[56] Ebd.
[57] Siehe dazu etwa *Stepanova,* Terrorism and Antiterrorism, in Kaldor/Rangelov (Hrsg.), The Handbook of Global Security Policy, S. 131; außerdem *Ramakrishna*, From ‚Old‘ to ‚New‘ Terrorism, in Gill (Hrsg.), Handbook of Security, S. 164.
[58] *Stepanova,* Terrorism and Antiterrorism, in Kaldor/Rangelov (Hrsg.), The Handbook of Global Security Policy, S. 130.
[59] *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 117; *Ramakrishna*, From ‚Old‘ to ‚New‘ Terrorism, in Gill (Hrsg.), Handbook of Security, S. 171.

Das weitverzweigte System eines Terrornetzwerks erstreckt sich über ganze Regionen und Kontinente, sodass eine Lokalisierung des Netzwerks und damit der Gefahrenquelle geradezu unmöglich ist. Hinzu kommt, dass der heutige Terrorismus im Cyberspace organisiert wird.[60] Das Internet bietet den Terrornetzwerken eine Vielzahl von verdeckten Kommunikations- und Organisationsmöglichkeiten. Dies erschwert die Arbeit der nationalen Sicherheitsorgane enorm.

Im Gegensatz zu ihren Vorläufern, verfolgen die modernen Terrororganisationen zudem häufig keine konkreten politischen oder nationalen Ziele, sondern basieren insbesondere auf ideologischen Vorstellungen. Ziel der Anschläge ist nicht mehr allein das Erregen von Aufmerksamkeit, die Kundgabe von politischen Überzeugungen sowie schließlich die Durchsetzung eben dieser politischen, revolutionäreren Interessen. Vielmehr legitimeren die Akteure ihre terroristischen Handlungen mit ideologischen Überzeugungen. Das Ziel ihrer Handlungen ist häufig die „Bestrafung“ von – aus deren Sicht – ideologisch fehlgeleiteten Regierungen und Bevölkerungen.[61] Die Ziele dieser Terrororganisationen sind nicht verhandelbar und so streben sie auch nicht nach Einigungen mit ihren Gegnern.[62] Auf Grundlage dieser Überzeugungen schrecken ideologische Terroristen nicht vor Massenmorden zurück und opfern dabei mutwillig ihr eigenes Leben im Wege ihrer Ideologie.[63]

Diese Strukturen des heutigen internationalen Terrorismus erschweren freilich auch die Gefahrenidentifizierung durch staatliche Sicherheitsbehörden. Zum einen ist aufgrund des globalen Netzwerks eine Lokalisierung der Gefahrenquelle äußerst schwierig. Zudem richten sich diese Terrororganisationen aufgrund ihres ideologischen Feindbildes nicht gegen bestimmte Staaten, sodass der territoriale Radius ihrer Terrorhandlungen häufig gerade nicht begrenzbar ist. Theoretisch kann jeder Staat, der nicht im Einklang mit den ideologischen Grundsätzen der Organisation steht, Ziel von Terroranschlägen werden. All diese Faktoren führen zu einer enormen Unberechenbarkeit.[64]

In jüngster Zeit hat sich diese Unberechenbarkeit sogar weiter zugespitzt. Es lässt sich ein Trend dahin erkennen, dass einzelne Individuen oder als kleine Terrorzellen zusammengeschlossene Individuen autonom Terroranschläge planen und ausführen, ohne Bestandteil eines organisierten Terrornetzwerks zu sein.[65] Auch

---

[60] *Andres*, National Security and U.S. Constitutional Rights, in Kulesza/Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance, S. 154.

[61] *Ramakrishna*, From ‚Old‘ to ‚New‘ Terrorism, in Gill (Hrsg.), Handbook of Security, S. 162; *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 118 ff.

[62] *Stepanova,* Terrorism and Antiterrorism, in Kaldor/Rangelov (Hrsg.), The Handbook of Global Security Policy, S. 131.

[63] *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 120; *Dearlove,* National Security and Public Anxiety, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence, S. 37.

[64] So auch *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 117.

[65] Siehe dazu auch *Stepanova,* Terrorism and Antiterrorism, in Kaldor/Rangelov (Hrsg.), The Handbook of Global Security Policy, S. 133; ebenso *Ramakrishna*, From ‚Old‘ to ‚New‘ Terrorism, in Gill

solche Individuen agieren auf Grundlage einer ideologischen Vorstellung. Diese Ideologie kann dabei durch Terrororganisationen motiviert sein, jedoch agieren diese Individuen völlig autonom. Gerade darin steckt die hohe Gefährlichkeit. So lässt sich in solchen Fällen nicht einmal ein bekanntes Netzwerk als Anknüpfungspunkt heranziehen. Bekannte Fälle dieser neuen Form des Terrorismus sind die Anschläge der rechtsextremen Terrorzelle NSU in Deutschland[66] oder die rechtsradikalen Attentate des Norwegers Anders Behring Breivik in Oslo und auf der Insel Utoya.[67] Auch die Anschläge junger Personen mit muslimischem Hintergrund, die unter dem Vorwand eines radikalen Glaubenskrieges und motiviert durch die Aufrufe des sogenannten IS, eine Reihe von Staaten durch Terrorangriffe erschüttert haben, sind Beispiele dieser Entwicklung.[68]

All diese Fälle haben gemeinsam, dass sie eigenständig, ohne direkte organisatorische Netzwerkbindung und unter einer ideologischen Vorstellung ausgeführt wurden. Wenn solche Individuen oder Terrorzellen nicht vorher schon den Sicherheitsbehörden auffallen, so ist die Verhinderung solcher Terrorangriffe nur erschwert möglich.

(Hrsg.), Handbook of Security, S. 174; *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik, S. 120.

[66] Der sogenannte „Nationalsozialistische Untergrund“ (NSU) war eine rechtsradikale Terrorzelle, die zwischen den Jahren 2000 und 2007 neun Personen mit Migrationshintergrund und eine Polizistin in Deutschland ermordet haben; siehe dazu *Fuchs/Goetz,* Die Zelle. Rechter Terror in Deutschland.

[67] Siehe dazu etwa *Jacobsen/Maier-Katkin,* Breivik's Sanity. Terrorism, Mass Murder, and the Insanity Defense. Dem Breivik-Attentat ist auch der jüngste rechtsextreme Anschlag auf 2 Moscheen in Christchurch (Neuseeland) vom 15. März 2019 sehr ähnlich, siehe dazu etwa *Pérez-Peña, Richard:* Two New Zealand Mosques, a Hate-Filled Massacre Designed for Its Time, The New York Times, 15.03.2019, abrufbar unter: https://www.nytimes.com/2019/03/15/world/australia/new-zealand-mosque-shooting.html?rref=collection%2Fspotlightcollection%2Fchristchurch-attack-new-zealand [zuletzt abgerufen: 01.12.2021].

[68] In diesen Fällen kann die Grenzziehung zwischen Einzelanschlägen von autonom agierenden Individuen, die lediglich durch den sog. IS motiviert wurden, und Attentaten, die direkt von der ISIS koordiniert und durchgeführt wurden, im Einzelfall schwierig sein. So war etwa die Anschlagsserie in Paris am 13.11.2015 ein koordinierter Terrorangriff einer Organisation, für die letztlich der sog. IS verantwortlich gemacht wurde. Dabei wurden an insgesamt 8 unterschiedlichen Orten in der Stadt – während eines Fußballspiels, in Cafés und Restaurants sowie während eines Konzerts – fast zeitgleich Sprengsätze detoniert und Stürmungen durch Terroristen, die mit Sturmgewähren bewaffnet waren, ausgeführt. Siehe hierzu *Wirtz/Harding,* Terroranschläge weltweit und in Europa, S. 557. Dahingegen waren die Anschläge beispielsweise in Nizza (2016), Berlin (2016) und Barcelona (2017), bei denen Einzeltäter mit großen Fahrzeugen in Menschenmengen rasten, zwar hinsichtlich des Anschlagsmusters geradezu identisch. Vgl. auch *Wirtz/Harding,* Terroranschläge weltweit und in Europa, S. 557 f. Allerdings lag hierbei eher eine Motivation der Täter durch die ISIS vor, während die Anschläge von ihnen wahrscheinlich autonom organisiert und ausgeführt wurden. Hinsichtlich des Attentäters von Berlin steht zumindest fest, dass Kontakte zur ISIS bestanden und somit eine ideologische Verbundenheit vorlag. Inwieweit sie indes organisatorisch in der Durchführung solcher Attentate involviert waren, ist unklar. Siehe dazu *Heil,* The Berlin Attack and the „Abu Walaa“ Islamic State Recruitment Network, S. 1 ff.

So kann resümierend an dieser Stelle festgestellt werden, dass die Beschaffung von Informationen über potenzielle Risiken, die Staatsinteressen tangieren können, als grundlegende Funktion der Geheimdienste im Laufe der Zeit zwar unverändert geblieben ist. Allerdings hat sich das Wesen der Risiken grundlegend geändert. Von einer klaren Gefährdungslage in früheren Zeiten hat sich die Gefahrenstruktur in der heutigen Welt in eine diffuse Situation gewandelt, wobei der moderne Terrorismus eine besondere Herausforderung für die staatliche Sicherheit darstellt. Im Zuge dieses Wandels haben sich die Mittel der geheimdienstlichen Arbeit gleichermaßen geändert. Die Verhinderung von modernen Terrorangriffen, die teilweise von einzelnen Individuen und Terrorzellen jederzeit aus der Mitte der Bevölkerung heraus geschehen können, ist für die Sicherheitsbehörden geradezu unmöglich. Dass hierfür ein Informationspool über die Telekommunikation zahlreicher Individuen und sogar ganzer Bevölkerungen für Ermittlungszwecke äußerst hilfreich ist, kann kaum geleugnet werden. Ob solche Massenüberwachungen allerdings auch mit den Menschenrechten der Individuen vereinbar sind, bleibt in den folgenden Abschnitten zu untersuchen.[69]

III. Die Informationsbeschaffung im geheimdienstlichen Arbeitsprozess

Die Strukturen und Methoden der geheimdienstlichen Informationsbeschaffung haben sich im Laufe der Geschichte erheblich fortentwickelt. Der Weg von den klassischen Nachrichtenbotschaften in der Antike, über die Entwicklung raffinierter mechanischer Spionageinstrumente im 19. und 20. Jahrhundert,[70] hin zu der heutigen digitalen Welt der Überwachung[71] belegt letztlich den unverkennbaren Modernisierungsprozess. Während in den antiken Großreichen etwa Königsboten und andere Beamte eingesetzt wurden, um Informationen über spezifische Nachrichtenwege den Herrschern zu übermitteln,[72] haben sich erst seit 1900 moderne technologiebasierte Geheimdienste entwickelt.

Der systematische Operationsprozess der heutigen Geheimdienste wird anhand des sogenannten *intelligence-cycle*[73] dargestellt, das die einzelnen Schritte des geheimdienstlichen Arbeitsprozesses und die Zusammenhänge innerhalb dieses Kreislaufs beschreibt. Dabei ist dieser Kreislauf nicht als starrer Arbeitsablauf zu verstehen, er stellt vielmehr eine systematische und vereinfachte Veranschaulichung von Grund-

---

[69] Siehe 2. und 3. Abschnitt.

[70] *Diffie/Landau,* Communications Surveillance. Privacy and Security at Risk, S. 42 f.

[71] Siehe dazu 1. Abschnitt, Unterabschnitt B. III. 2. Im 2. und 3. Abschnitt werden die heutigen Methoden der Telekommunikationsüberwachung menschenrechtlich untersucht.

[72] *Krieger*, Geschichte der Geheimdienste, S. 21 ff.

[73] *Blancke*, Geheimdienste und Globalisierte Risiken, S. 19; *Müller*, Strategischer Nachrichtendienst und Informationsmanagement?, in Zoller/Korte (Hrsg.), Nachrichtendienste in der Informationsgesellschaft, S. 35; *Lowenthal*, From Secrets to Policy, S. 70, 84, Lowenthal bezeichnet den Prozess als „*intelligence process*“.

zügen der internen Prozessabläufe und -mechanismen eines modernen Geheimdienstes dar.[74]

Im ersten Schritt der Planung (*Planning and Direction*), die den geheimdienstlichen Arbeitsprozess in Gang setzt, werden die Ziele und Prioritäten des Prozesses definiert.[75] Diese ergeben sich aus Fragestellungen, Befürchtungen oder konkreten Erwägungen,[76] die die staatlichen Entscheidungsträger auf Grundlage politischer oder wirtschaftlicher Entwicklungen und Geschehnisse formulieren.[77]

Relevante Informationen, die diese Ziele und die entsprechenden Fragestellungen betreffen, werden anschließend gesammelt (*Collection*).[78] Die Methoden der Informationsbeschaffung sind indes zahlreich und werden in der geheimdienstlichen Terminologie unter den sog. „*Ints*" zusammengefasst.[79] Nachdem die gesammelten Informationen aufgeschlüsselt und aufgearbeitet wurden (*Processing*),[80] folgt im Zuge der vierten Station die Analyse und Auswertung der Informationen (*Analysis*). Hier kristallisiert sich letztlich heraus, inwieweit die beschafften Informationen die zu Beginn formulierten Fragen beantworten.[81] So zeigt sich hier beispielsweise, ob die Informationen etwa Aufschluss über den Aufenthaltsort eines gesuchten Terroristen geben oder ob eine konkrete terroristische Bedrohung bevorsteht. Schließlich werden die Ergebnisse der Analyse den politischen Entscheidungsträgern weitergeleitet (*Dissemination*).[82] Auf Grundlage dieser Informationen können nun politische Entscheidungen getroffen werden. Dieser Schritt kann indes Anlass geben für weitere Fragen und Befürchtungen, die letztlich den Prozesskreislauf erneut in Gang setzen können.

Für die vorliegende Untersuchung ist die Informationsbeschaffung als eine Station dieses Arbeitsprozesses von besonderem Interesse. Denn die zentrale

---

[74] Teilweise wird diese Vereinfachung kritisiert, so etwa *Omand,* The Cycle of Intelligence, in Dover/Goodman/Hillebrand (Hrsg.), Routledge Companion to Intelligence Studies, S. 63.

[75] Vgl. *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 12–13; *Lowenthal*, From Secrets to Policy, S. 70 f.

[76] Dies können allgemeine Fragen beispielsweise zu der militärischen Ausrüstung eines bestimmten Landes sein oder ebenso eine konkrete Frage etwa nach dem Aufenthaltsort eines gesuchten Terroristen. Siehe dazu etwa *Blancke*, Geheimdienste und Globalisierte Risiken, S. 19; außerdem *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 12–13; *Omand,* The Cycle of Intelligence, in Dover/Goodman/Hillebrand (Hrsg.), Routledge Companion to Intelligence Studies, S. 68.

[77] *Lowenthal*, From Secrets to Policy, S. 87 ff.

[78] Siehe *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 15.

[79] Näheres zu den Methoden der geheimdienstlichen Informationsbeschaffung im 1. Abschnitt, Unterabschnitt B. III. 1.

[80] Überwiegend wird der Schritt „*Processing*" als separate Station in dem Prozess aufgeführt, siehe etwa: *Johnson:* National Security Intelligence, in Johnson (Hrsg.): The Oxford Handbook of National Security Intelligence, S. 19; *Lowenthal*, From Secrets to Policy, S. 77 f.

[81] *Omand,* The Cycle of Intelligence, in Dover/Goodman/Hillebrand (Hrsg.), Routledge Companion to Intelligence Studies, S. 69.

[82] *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 21.

Fragestellung dieser Dissertation ist, ob und inwieweit die geheimdienstliche Praxis der Telekommunikationsausspähung mit dem internationalen Menschenrechtsschutz vereinbar ist. Vor diesem Hintergrund wird im Folgenden nach einem Überblick über die geheimdienstlichen Methoden zur Informationsbeschaffung der Fokus auf die heutige Praxis der Telekommunikationsausspähung gerichtet.

1. Methoden der geheimdienstlichen Informationsbeschaffung

Ausgehend von der geheimdienstlichen Vorgehensweise werden die Methoden zur Beschaffung relevanter Informationen unter den sogenannten „*Ints*" kategorisiert.[83] Zwar stammt diese Kategorisierung aus den USA, allerdings sind die hierunter gefassten Methoden als solche in der geheimdienstlichen Praxis zahlreicher Nationen vorzufinden.[84] Letztlich wird mithilfe dieser Systematisierung die Bandbreite der Spionagemethoden kategorisiert. Zugleich spiegelt sich der bereits angedeutete historische Entwicklungsprozess der Instrumentarien geheimdienstlicher Informationsbeschaffung in den „*Ints*" wider.[85]

So ist das älteste Mittel der Informationssammlung der Einsatz von Menschen, die als klassische Spione Informationen einholen und weisungsgemäß übermitteln. Diese im System der „*Ints*" als *HUMINT – Human Intelligence* – bezeichnete Methode umschreibt letztlich die typische Tätigkeit des gemeinhin bekannten geheimdienstlichen Agenten. Diese ursprünglichste Form der Spionage bildet die Wurzel des heute weit verzweigten Operationsspektrums moderner Geheimdienste. Nicht grundlos wird die Tätigkeit der Spionage als „*second oldest profession*" bezeichnet.[86] Was damals im Kontext der noch aufkeimenden Strukturen eines antiken Staatswesens einfache Königsboten erledigten, wird heute von speziell ausgebildeten Agenten ausgeführt.[87] Der Einsatz von menschlichen Spionen ist in vielen Bereichen allmählich durch effektivere technologische Instrumente abgelöst worden, dennoch ist *HUMINT* auch heute noch ein sehr wichtiges Mittel im geheimdienstlichen Instrumentarium.[88] Insbesondere zur Ermittlung konkreter Informationen, die durch technische Mittel nicht zu erfassen sind, ist der Einsatz von Spionageagenten unverzichtbar.[89] Dabei agieren heute Agenten verdeckt, indem sie mit einer fiktiven

[83] *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 15 ff.
[84] Siehe hierzu etwa: *Blancke*, Geheimdienste und Globalisierte Risiken, S. 18; *Lowenthal*, From Secrets to Policy, S. 87. Da die *Intelligence*-Forschung ihre Wurzeln in den USA hat, stammen die theoretischen Ansätze in diesem Forschungsfeld überwiegend aus den USA.
[85] *Blancke*, Geheimdienste und Globalisierte Risiken, S. 18.
[86] *Knightley*, The Second Oldest Profession; *Lowenthal*, From Secrets to Policy, S. 127.
[87] Die spezielle Ausbildung umfasst dabei mehrere Jahre; *Lowenthal* zufolge sind es durchschnittlich sieben Jahre in den USA, siehe *Lowenthal*, From Secrets to Policy, S. 129.
[88] *Johnson*, Secret Agencies, S. 19.
[89] *Lowenthal*, From Secrets to Policy, S. 132; Zieht sich eine terroristische Vereinigung etwa in abgelegenen Territorien zurück und nutzen diese bewusst Kommunikationsmethoden, die technisch nicht

Identität unter dem Anschein eines durchschnittlichen Lebens mit einem üblichen Beruf und sogar in einer Familie lebend besonders im Ausland, aber auch im Inland, den geheimdienstlichen Aufträgen geheim nachgehen.[90]

In Abgrenzung zu *HUMINT* wird mit dem Oberbegriff *TECHINT – Technical Intelligence* – der Einsatz von technischen Überwachungsmitteln, die im Zuge des technologischen Fortschritts entwickelt wurden, umschrieben.[91] Unter *TECHINT* fallen insbesondere *IMINT* und *SIGINT*. So ist *IMINT* (*Imagery Intelligence*) eine Methode zur Beschaffung von Informationen in Form von Bildern,[92] wobei mithilfe von fototechnischen Systemen Aufnahmen von konkreten Objekten aus der Distanz erstellt werden. So kann das Zielobjekt etwa eine Stadt sein, sodass bildliche Aufnahmen Informationen über die Infrastruktur, der Bebauung oder den natürlichen Gegebenheiten liefern.[93] Weiterhin sind ebenso gezielte Aufnahmen einzelner Areale oder konkreter Gebäudekomplexe möglich. Bereits während der beiden Weltkriege wurden aus Flugzeugen fotografische Aufnahmen gewonnen.[94] Zwar werden auch heute noch Flugzeuge einge-setzt, allerdings überwiegt nun der Einsatz von Satelliten,[95] die digitales Bildmaterial aufnehmen und an Empfangsstationen auf der Erde transferieren.[96] Auch unbemannte Drohneneinsätze bieten den Geheimdiensten heute entscheidende Vorteile. So werden solche Drohnen aus der Ferne gesteuert, sodass etwa eigene Soldaten keinen direkten Risiken mehr ausgesetzt sind. Zudem können sie durch modernste Technologien Echtzeitaufnahmen liefern, die eine zeitgleiche Analyse und Bearbeitung aus der Ferne ermöglichen.[97] Die Bilder und graphischen Darstellungen, die auf dem Wege dieser Beschaffungsmethode gewonnen werden, verschaffen einen umfassenden Überblick über Städte und Areale und können so je nach geheimdienstlichem Auftrag detaillierte

---

ausgespäht werden können, kann ein eingeschleuster Geheimdienstagent, der das Vertrauen der Gruppe genießt, theoretisch viele Informationen sammeln. In der Praxis sind solche Aktionen sicherlich nicht ungefährlich, denn eine Entlarvung des Agenten ist nie auszuschließen. Dabei wird Spionage durch einen Agenten als politisches Delikt in zahlreichen Staaten ernsthaft geahndet. Siehe dazu: *Lowenthal*, From Secrets to Policy, S. 133 ff. In Deutschland steht die geheimdienstliche Agententätigkeit gem. § 99 StGB unter Strafe.

[90] *Lowenthal*, From Secrets to Policy, S. 129 f.

[91] *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 17.

[92] Imint wird teilweise auch Geoint (Geospatial Intelligence) sowie Photint (Photo Intelligence) genannt.

[93] *Lowenthal*, From Secrets to Policy, S. 107; *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 84.

[94] Ebd., S. 83; *Lowenthal*, From Secrets to Policy, S. 107.

[95] Immer mehr Staaten verfügen über staatseigene Satelliten oder entwickeln solche. Zudem pflegen viele Staaten auf diesem Gebiet Kooperationen mit verbündeten Staaten. Aber auch der Erwerb von Aufnahmen, die von kommerziellen Unternehmen produziert werden, ist heutzutage nicht unüblich, siehe dazu: *Lowenthal*, From Secrets to Policy, S. 111 f.; Sowie *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 83.

[96] Ebd., S. 83.

[97] *Lowenthal*, From Secrets to Policy, S. 112.

Informationen liefern. Dabei kann sowohl eine einzige Aufnahme aufschlussreiche Informationen über den Ist-Zustand eines Objekts liefern. Darüber hinaus können ganze Aufnahmereihen indes Entwicklungen und Bewegungen in einem bestimmten Objekt – etwa in einem Krisengebiet – dokumentieren.[98]

Eine weitere technologische Methode der Informationsbeschaffung ist *SIGINT* (*Signals Intelligence*). Hierbei handelt es sich um die Erfassung von elektronischen Signalen durch Satelliten sowie spezielle erdgebundene Auffangeinrichtungen. Insbesondere umfasst diese Methode auch die klassische Fernmeldeaufklärung, d.h. die Ausspähung der Telekommunikation. In der geheimdienstlichen Terminologie wird diese spezielle Form von *SIGINT* auch *COMINT* (*Communications Intelligence*) bezeichnet.[99] Die Methoden der Telekommunikationsausspähung werden im folgenden Unterkapitel indes näher hinterleuchtet.

Schließlich beschaffen Geheimdienste Informationen ferner aus offenen Quellen. Diese als *OSINT* – *Open Source Intelligence* – bezeichnete Form der Informationsbeschaffung mag bereits begrifflich paradox wirken.[100] Tatsächlich wird jedoch ein weiter Teil der Informationen aus allgemein zugänglichen Quellen gewonnen.[101] Als solche Quellen kommen Medien wie Zeitungen, Fernsehen oder Internet, aber auch Regierungserklärungen, öffentliche Reden von Politikern, zudem akademische Zeitschriften und Konferenzen in Betracht.[102] Insbesondere in der heutigen Welt der Informationstechnologie ist die Menge öffentlicher Informationen im Internet unüberschaubar. Insofern stellt der Zugang zu diesen Informationen zwar kein Problem dar, allerdings muss ein Geheimdienst relevante Informationen zunächst aus dieser Fülle an Daten herausfiltern.[103] Die wohl modernste Untergruppe der *OSINT* ist *SOCMINT* – *Social Media Intelligence*. Darunter ist die Gewinnung von offenen Informationen aus sozialen Medien wie *Facebook*, *Twitter* oder *Instagram* zu verstehen.[104]

[98] *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 84.
[99] *Lowenthal*, From Secrets to Policy, S. 118.
[100] So ist die Bezeichnung dieser Form der Informationsgewinnung als „geheimdienstliche Beschaffungsart" nicht gänzlich unumstritten, siehe dazu *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 85–87 m.w.N.; außerdem *Hulnick,* The Dilemma of Open Sources Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence, S. 230 ff.
[101] *Lowenthal*, From Secrets to Policy, S. 137.
[102] Ebd.
[103] Ebd., S. 139.
[104] Siehe dazu beispielsweise die Homepage des BND, in der *SOCMINT* als nachrichtendienstliches Mittel zur Informationsgewinnung genannt wird: https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html [zuletzt abgerufen 01.12.2021].

2. Die Telekommunikationsausspähung

Historisch zurückgehend auf den ersten Weltkrieg,[105] spielt *COMINT* heute in der geheimdienstlichen Informationsbeschaffung eine bedeutende Rolle.[106] So eröffnet die Telekommunikationsausspähung einen äußerst informativen – und von den betroffenen Parteien unbemerkten – Einblick in einen persönlichen Dialog. Der Geheimdienst kann hierdurch beispielsweise in Erfahrung bringen, welche Aktionen von mutmaßlichen Tätern zukünftig geplant werden. Neben einer reinen Inhaltsanalyse können indes auch sonstige Metadaten, so etwa die Häufigkeit oder der Ort der Kommunikation zwischen zwei Personen, aufschlussreich sein. Die Analyse von Telekommunikations-Metadaten wird auch *traffic analysis* genannt.[107] Dabei ist die Bandbreite der verfügbaren Kommunikationsdaten mit dem Fortschritt der Telekommunikationstechnologie enorm gewachsen. Neben klassischen Telefonaten oder Faxen, haben sich heute weltweit auch internetbasierte Nachrichtensysteme zum persönlichen Informationsaustausch etabliert. Dazu gehören Emails, Internet-Telefonie sowie insbesondere sog. *Instant Messanger* wie beispielsweise *WhatsApp*, *Skype* oder *Telegram*.[108] Die moderne Kommunikationstechnologie bietet den Geheimdiensten letztlich einen unerschöpflichen Informationspool an. Die Geheimdienste reagieren indes auf informationstechnische Entwicklungen im Bereich der Telekommunikation und optimieren ihre Methoden zur Erfassung dieser enormen Datenmengen.[109]

So haben sich die Methoden der Telekommunikationsausspähung im Laufe der Zeit weiterentwickelt. In den vergangenen Jahren haben insbesondere Enthüllungen offengelegt, wie die Geheimdienste die Telekommunikation von Individuen ausspähen. Ausgehend von der Art des Zugangs zu den Kommunikationsdaten, lassen sich die modernen Formen der Telekommunikationsüberwachung drei Hauptkategorien zusammenfassen:[110]

1. Der Geheimdienst entnimmt Daten aus Servern von privaten Service Providern;
2. Der Geheimdienst greift direkt auf Telekommunikationsnetzwerke zu;
3. Der Geheimdienst verschafft sich Zugriff auf private Telekommunikationsgeräten.

---

[105] *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 80; *Ferris,* Signals Intelligence in War and Power Politics, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence, S. 156.

[106] *Lowenthal*, From Secrets to Policy, S. 119.

[107] Ebd.

[108] Ebd., S. 120; siehe auch *Jakob*, Geheime Nachrichtendienste und Globalisierung, S. 80.

[109] *Ferris,* Signals Intelligence in War and Power Politics, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence, S. 156.

[110] So gliedert auch *Lyon,* Surveillance after Snowden, S. 21 f.

a. Zugriff auf das Telekommunikationsnetzwerk während der Datenübertragung

Die moderne Kommunikationsinfrastruktur basiert überwiegend auf einem globalen Netz von zahlreichen Datenkabeln, die die einzelnen Kontinente weltumspannend miteinander verbinden und damit das Telefon- und Internetnetzwerk der heutigen Zeit möglich machen.[111] Untersee-Glasfaserkabel ermöglichen eine High-Speed-Übertragung von Telekommunikationsdaten. In diesen Lichtwellenleitern werden die Daten als Lichtimpulse fast mit Lichtgeschwindigkeit über weite Distanzen hinweg transportiert.[112] Somit fließt eine unvorstellbar große Datenmenge ununterbrochen durch das gesamte globale Netzwerk. Dabei werden die Daten nicht notwendigerweise auf dem kürzesten Weg übertragen. Vielmehr werden die Datenpakete über die schnellsten und günstigsten Übertragungswege zum Empfänger übermittelt. So können die Datenpakete durchaus grenzüberschreitend global unterwegs sein, obwohl sich Absender und Empfänger innerhalb eines Staates befinden.[113]

Mithilfe technischer Vorrichtungen können Geheimdienste direkt auf das Telekommunikationsnetzwerk zugreifen und die Kommunikationsdaten auf dem Übertragungsweg vom Absender zum Empfänger unbemerkt abfangen. Seitdem die weltweite Telekommunikation zunehmend über Lichtsignale durch Untersee-Glasfaserkabel fließt, haben die Geheimdienste einzelner Staaten Spionage-U-Boote zum Anzapfen dieser Kabel eingesetzt.[114] Techniker der Geheimdienste können in Untersee Glasfaserkabel auftrennen und sogenannte Kabelteiler („*splitter*“) anbringen. Der durchfließende Datenverkehr wird durch diese Geräte kopiert und an die Datenspeicherplätze des Geheimdienstes umgeleitet.[115] Einerseits können so etwa Telefongespräche in Echtzeit abgehört sowie Emails und andere private Nachrichten

[111] Die Webseite http://www.submarinecablemap.com/ [zuletzt abgerufen 01.12.2021] gibt einen Überblick über das globale Unterwasserkabel-Netzwerk. Alle aktuellen Trassen, Landungs- und Endstellen sind hier auf einer Weltkarte markiert und verdeutlichen die enorme Vernetzung, auf die unsere heutige Internet-Gesellschaft basiert.

[112] Siehe dazu bereits einen Beitrag von 1989: *Preissner-Polte*: Wie der Blitz; vgl. außerdem https://www.netzwerke.com/allgemein/was-leisten-glasfaserkabel-in-modernen-netzwerken.html# [zuletzt abgerufen 01.12.2021].

[113] *Landau,* Surveillance or Security?, S. 71; Siehe auch EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 14.

[114] So hat etwa der US-Geheimdienst „NSA“ U-Boote eingesetzt; vgl. dazu etwa *Meister, Andre*: Glasfaserkabel und Spionage-U-Boote. Wie die NSA die Nervenzentren der Internet-Kommunikation anzapft, 20.06.2013 https://netzpolitik.org/2013/glasfaserkabel-und-spionage-u-boote-wie-die-nsa-die-nervenzentren-der-internet-kommunikation-anzapft/ [zuletzt abgerufen 01.12.2021].

[115] *Bowden,* Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger, S. 16; *Zetter, Kim:* What We Know About the NSA and AT&T’s Spying Pact, 10.08.2015, abrufbar unter https://www.wired.com/2015/08/know-nsa-atts-spying-pact/ [zuletzt abgerufen 01.12.2021]. Siehe auch ZDNet: https://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/ [zuletzt abgerufen 01.12.2021].

gespeichert werden.[116] Darüber hinaus gelangen die Metadaten über jegliche Korrespondenzen, die über die Datenkabelverbindungen zustande kommen, in die Hände der Geheimdienste.[117] In den Quartieren der Geheimdienste werden die abgefangenen Daten häufig zunächst zwischengespeichert. Zur Reduzierung des enormen Datenvolumens werden die „wichtigen" Informationen durch spezifische Computerprogramme herausgefiltert. Mithilfe zuvor festgelegter Suchbegriffe, die auch bestimmte Emailadressen oder Telefonnummern umfassen können, werden die Daten zumeist anschließend – ausgehend von den Zielen der geheimdienstlichen Überwachung – auf verdächtige Indizien durchsucht.[118]

Unter dem Operationsnamen „*TEMPORA*" hat der britische Geheimdienst GCHQ etwa Datenströme aus transatlantischen Glasfaserkabelverbindungen unbemerkt angezapft und Telekommunikationsdaten von unzähligen Individuen über einen längeren Zeitraum gespeichert. Die Daten wurden anschließend nach geheimdienstlich interessanten Informationen gefiltert und sodann analysiert. Dabei wurden sowohl Inhalte aus Emails, Telefongesprächen und *Facebook*-Einträgen als auch Metadaten – etwa über Identität und Standort der Internetnutzer – abgefangen.[119] Der US-Geheimdienst NSA hatte umfassenden Zugang zu den Daten. Diese eigentlich geheime Operation des GCHQ wurde im Zuge der *Snowden*-Enthüllungen bekannt und ist Gegenstand der Entscheidung *Big Brother Watch and Others v. The United Kingdom* des EGMR.[120] Auch das vom US-Geheimdienst NSA operierte Programm „*UPSTREAM*" umfasst eine weitreichende Datenausspähung aus Glasfaserverbindungen.[121]

---

[116] So wurden etwa im Rahmen des NSA-Programms „*Stellar Wind*", das durch *Whistle-Blower* bekannt wurde, nahezu alle Emails, die in den USA unterwegs waren, abgefangen. Auch unter dem durch *Edward Snowden* bekannt gewordene Programm „*UPSTREAM*" wurden unzählige Emails und andere digitale Korrespondenzformen abgefangen. Siehe dazu *Clement/Obar:* Canadian Internet „Boomerang" Traffic and Mass NSA Surveillance, in Geist (Hrsg.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era, S. 18.

[117] *McAskill, Ewen u.a.,* „GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications" The Guardian, 21. Juni 2013, abrufbar unter http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [zuletzt abgerufen 01.12.2021].

[118] Siehe dazu auch *Georgieva,* The Right to Privacy under Fire, S. 107; *Schaller*, Strategic Surveillance and Extraterritorial Basic Rights Protection, S. 945.

[119] *McAskill, Ewen u.a.,* „GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications" The Guardian, 21. Juni 2013, abrufbar unter http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [zuletzt abgerufen 01.12.2021]. Siehe außerdem EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 17.

[120] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021. Sie ist auch Gegenstand in den noch anhängigen Beschwerden *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* [Communicated Case], Rs. 62322/14, 5. Januar 2015 sowie *10 Human Rights Organisations and Others v. the United Kingdom* [Communicated Case], Rs. 24960/15, 24. November 2015.

[121] EGMR, *Big Brother Watch and Others v. The United Kingdom* [First Section], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 25.

Ein weiterer Eingriff in das Kommunikationsnetzwerk erfolgt beispielsweise durch die Ausspähung von Mobilfunk durch sogenannte IMSI-Catcher.[122] Dazu werden diese Catcher installiert, die die Mobilfunk-Basisstation von Netzbetreibern simulieren. Der IMSI-Catcher täuscht vor, die Basisstation eines Netzbetreibers zu sein, wobei ein IMSI-Catcher im Gegensatz zu den regulären Mobilfunk-Basisstationen deutlich höhere Empfangsleistungen haben. Mobiltelefone verbinden sich automatisch mit einer Basisstation in der Umgebung, die die bessere Empfangs- und Sendeleistung hat. Infolgedessen stellen alle Mobiltelefone in der Umgebung eines IMSI-Catchers nun aufgrund der höheren Empfangsleistung eine Verbindung zu diesen Catchern auf, anstatt Signale an die reguläre Basisstation des Netzbetreibers zu schicken.[123] Die Operatoren der Catcher haben anschließend Zugang zu allen Daten, die auf dem Mobilfunkgerät gespeichert sind. Auch die Gespräche über das Mobiltelefon können verfolgt und abgehört werden.[124] Da bei diesem Eingriff in das Telekommunikationsnetzwerk zugleich der Zugang zu einzelnen Mobiltelefonen ermöglicht wird, fällt diese Eingriffsform auch unter die Fallgruppe des geheimdienstlichen Zugriffs auf private Telekommunikationsgeräte.[125]

b. Beschaffung von Telekommunikationsdaten aus Servern von *Service Providern*

Mithilfe moderner Kommunikationstechnologien können Individuen sekundenschnell, häufig kostenlos und in höchster Qualität miteinander kommunizieren und damit weite Distanzen unkompliziert überbrücken. Telekommunikations- und Internetdienstleister (sog. *Service Provider*) bieten dabei ein weites Spektrum an Korrespondenzmöglichkeiten an, die weltweit von unzähligen Individuen genutzt werden.[126] Dementsprechend sind Menge und Vielseitigkeit der Benutzer- und Verbindungsdaten auf den Servern der *Service Provider* unübertrefflich hoch. Angesichts dessen ist es nicht verwunderlich, dass führende *Service Provider* für Geheimdienste eine wertvolle Informationsquelle darstellen. So ist bekannt, dass Geheimdienste Kommunikationsdienstleister zur Herausgabe von Benutzerdaten auffordern oder sogar auf Grundlage gesetzlicher Regelungen oder richterlicher Anordnungen direkten Zugang zu den Servern von *Service Providern* haben.[127] So erhalten die Geheimdienste unmittelbaren Zugriff auf alle Daten, die auf den Servern der *Service Providern* gespeichert sind. Sowohl die Metadaten jeglicher Verbindungen und

---

[122] Siehe dazu am Beispiel des § 100i StPO in Deutschland *Keller/Braun/Hoppe,* Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, S. 63 f.

[123] *Keller/Braun/Hoppe,* Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, S. 65. Siehe außerdem *Keller,* Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit, S. 43 ff.

[124] *Ney/Smith/Cadamuro/Kohno*, SeaGlass. Enabling City-Wide IMSI-Catcher Detection, S. 39 f.

[125] Siehe nachfolgenden Unterabschnitt B. III. 2. c.

[126] Siehe dazu bereits 1.Abschnitt, Unterabschnitt A. II.

[127] Siehe 2. Abschnitt, Unterabschnitt B. I. 1. b.

Internetanfragen als auch alle Inhalte, wie etwa Emails, Chats, Datentransfers und andere Korrespondenzen befinden sich dadurch in den Händen der Geheimdienste.[128]

Ein besonders weitreichendes Beispiel dieser Form der Telekommunikationsausspähung ist das vom US-Geheimdienst NSA eingesetzte Überwachungsprogramm „*PRISM*“, das ebenfalls im Zuge der *Snowden*-Enthüllungen bekannt wurde.[129] Im Rahmen dieses Überwachungsprogramms müssen die bekannten *Service Provider Google*, *YouTube*, *Facebook*, *Microsoft*, *Skype*, *PalTalk*, *AOL*, *Yahoo* und *Apple* dem US-Geheimdienst NSA auf Grundlage von entsprechenden Beschlüssen des *Foreign Intelligence Surveillance Court* (FISC) direkten Zugriff auf Ihren Servern gewähren. Diese Praxis basiert auf dem *Foreign Intelligence Surveillance Act* (FISA). Dieses Gesetz regelt unter anderem die Telekommunikationsüberwachung von Personen, die außerhalb des Territoriums der USA leben, und von US-Bürgern, die mit Personen außerhalb der USA kommunizieren.[130]

Die *Service Provider* können auch im Rahmen von nationalen Regelungen zur Vorratsdatenspeicherung zur Quelle der geheimdienstlichen Informationsgewinnung werden. Telekommunikationsdienstleister werden hierbei aufgrund von Gesetzen verpflichtet, sämtliche Verbindungsdaten von Telekommunikationen der Nutzer für einen bestimmten Zeitraum auf Vorrat zu speichern. Staatliche Institutionen – insbesondere Strafverfolgungsorgane und Geheimdienste – können im Bedarfsfall für Ermittlungszwecke oder zur präventiven Gefahrenabwehr auf diese Daten zurückgreifen.[131] Aufgrund einer solchen Regelung wird sichergestellt, dass alle Internetdienstleister Daten speichern und bei Bedarf herausgeben müssen. Würden etwa einige *Service Provider* aufgrund eines unternehmerischen Treue- und Moralkodexes gegenüber ihren Kunden auf jegliche Kooperationen mit Geheimdiensten kategorisch verzichten, so wären sie jedoch bei geltenden Gesetzen zur Vorratsdatenspeicherung hierzu unausweichlich verpflichtet. Somit erweitern Vorschriften zur Vorratsdatenspeicherung den Kreis der *Service Provider*, die den Geheimdiensten als Informationsquelle dienen.

Gerade in Europa hat die Vorratsdatenspeicherung in den letzten Jahren für viele Diskussionen gesorgt. So hat einerseits eine im Jahr 2006 erlassene EU-Richtlinie zur Vorratsdatenspeicherung die EU-Mitgliedstaaten dazu verpflichtet, diese Richtlinie und damit die Praxis der Datenspeicherung in nationales Recht

---

[128] *Georgieva,* The Right to Privacy under Fire, S. 107.

[129] *Greenwald, Glenn and McAskill, Ewen* „NSA Prism Program Taps in to User Data of Apple, Google and Others“ The Guardian 7. Juni 2013, abrufbar unter http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link [zuletzt abgerufen 01.12.2021].

[130] Ebd.; EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 23.

[131] *Moser-Knierim,* Vorratsdatenspeicherung, S. 140. Außerdem Office of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age: Report of the OHCHR, A/HRC/39/29, 03. August 2018, Rn. 18.

umzusetzen.[132] Allerdings hat der EuGH eben diese Richtlinie acht Jahre später aufgrund von Unionsrechtswidrigkeit für ungültig erklärt.[133] Dabei wurden in der Zwischenzeit aufgrund der Umsetzungspflicht in vielen europäischen Ländern Gesetze zur Vorratsdatenspeicherung erlassen.[134] Die Verfassungsgerichte vieler Staaten haben jedoch die Verfassungswidrigkeit der Regelungen festgestellt, und zwar viele bereits vor der Ungültigkeitsentscheidung des Europäischen Gerichtshofs.[135]

c. Zugriff auf private Telekommunikationsgeräte

Schließlich können sich Geheimdienste direkt in privatgenutzte Telekommunikationsgeräte einhacken, um sich auf diesem Weg umfassenden Zugriff auf die Kommunikation einer bestimmten Person, die über das Zielgerät erfolgt, zu verschaffen.[136] Dadurch können Kommunikationsvorgänge erfasst werden, ohne dass es einer komplizierten Entschlüsselung der üblicherweise End-to-End-verschlüsselten Telekommunikation bedarf.[137] Im Vordergrund dieser Form der Telekommunikationsausspähung stehen spezielle Schadprogramme („*Malware*"), die zu diesem Zweck in private Mobiltelefone oder Computer eingeschleust und installiert werden.[138] Es gibt eine Vielzahl unterschiedlicher Schadprogramme, die nach Ihrer Funktionalität klassifiziert werden.[139] Einige dieser *Malwares* ermöglichen einen Fremdzugriff auf die Dateien, die sich auf dem infizierten Computersystem befinden. Sogenannte „Trojaner" haben äußerlich eine nützliche Funktion, verursachen aber im Hintergrund aufgrund eines verstecken Codes Schaden für das System.[140]

---

[132] Am 15. März 2006 ist die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten (Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG) in Kraft getreten.

[133] EuGH, *Digital Rights Ireland und Seitlinger*, Rs. C-293/12,8. April 2014. In Deutschland hat indes das BVerfG bereits am 2. März 2010 die zur Umsetzung der EU-Richtlinie verabschiedeten nationalen Gesetze zur Vorratsdatenspeicherung als verfassungswidrig aufgehoben, siehe BVerfGE 125, 260–385.

[134] Ausführlich dazu *Moser-Knierim,* Vorratsdatenspeicherung, S. 169.

[135] So etwa das BVerfG zur deutschen Regelung, siehe BVerfGE 125, 260–385. Siehe außerdem *Moser-Knierim,* Vorratsdatenspeicherung, S. 170.

[136] Siehe dazu auch *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 113ff. Außerdem Office of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age: Report of the OHCHR, A/HRC/39/29, 03. August 2018, Rn. 19.

[137] *Biselli, Anna*: Deutschland hält an widersprüchlicher Kryptopolitik fest und gefährdet vertrauliche Kommunikation für alle, 28.10.2016, abrufbar unter https://netzpolitik.org/2016/deutschland-haelt-an-widerspruechlicher-kryptopolitik-fest-und-gefaehrdet-vertrauliche-kommunikation-fuer-alle/ [zuletzt abgerufen 01.12.2021].

[138] Der britische Geheimdienst GCHQ hat etwa über verfälschte LinkedIn-Seiten den Upload von Malware auf private Computersysteme durch arglose Personen bewirkt, siehe dazu https://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html [zuletzt abgerufen 01.12.2021].

[139] *Kappes,* Netzwerk- und Datensicherheit, S. 95.

[140] Ebd.

„*Spyware*" sammeln ohne Wissen und Einverständnis des Benutzers Informationen, die sich auf dem Telekommunikationsgerät befinden, oder zeichnen die Maus und Tastatureingaben im Gerät durch sogenannte *Keylogger* auf und leiten diese an Dritte weiter.[141] Eine weitere Form von Schadprogrammen namens „*Backdoors*" verändert Programme auf einem System und ermöglicht unter Umgehung der auf dem Computersystem installierten Sicherheitsmechanismen den Fremdzugriff auf das System.[142]

Durch das Einschleusen solcher Programme sind einerseits die auf dem Kommunikationsgerät gespeicherten Emails und Nachrichten einsehbar.[143] Zudem können auch alle Aktivitäten in Echtzeit beobachtet werden. Schreibt eine Person mit einem infizierten Computer etwa eine E-Mail, so kann diese mithilfe der entsprechenden Software eingesehen werden, schon bevor die E-Mail überhaupt versendet wird. Darüber hinaus gewinnen Geheimdienste auf diesem Weg auch Zugriff auf integrierte Kameras und Mikrofone, sodass beispielsweise Videochats oder Telefonate in Echtzeit abgehört werden können.[144] Diese Form der Ausspähung geschieht im Hintergrund und wird vom Nutzer in der Regel nicht bemerkt.

Durch die Installation von Funkwanzen können zudem private Computer ausgespäht werden, ohne dass es einer Internetverbindung bedarf. Die Sender werden entweder in einem Rechner eingebaut oder sind in USB-Sticks versteckt. Über eine Radiofrequenz können die Daten heimlich an Abhörstationen der Geheimdienste übertragen werden.[145]

---

[141] Ebd.; *Weber/Staiger*, Privacy versus Security, in Kulesza/Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance, S. 76.

[142] Ebd., S. 96.

[143] Beim sog. „Daten-Monitoring" werden kontinuierlich in regelmäßigen Zeitabständen die im Computersystem gespeicherten Daten gespiegelt und Änderungen erfasst. Damit kann im Laufe der Zeit anhand der so erfassten Daten ein komplettes Profil über das IT-Verhalten des Anwenders gewonnen werden. Vgl. etwa *Buermeyer,* Die „Online-Durchsuchung", S. 160 f.

[144] Siehe dazu *Buermeyer,* Die „Online-Durchsuchung", S. 161 f.

[145] Laut einem Bericht der New York Times hat etwa der US-Geheimdienst NSA über 100.000 Computer mit solchen Spionagesystemen ausgestattet. *Sanger, David E/Shanker, Thom*: N.S.A. Devises Radio Pathway into Computers, The New York Times, 15. Januar 2014, abrufbar unter http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html [zuletzt abgerufen 01.12.2021].

2. Abschnitt: Geheimdienstliche Telekommunikationsüberwachung innerhalb des Staatsgebiets

Die moderne Telekommunikationsüberwachung durch Geheimdienste dient dem staatlichen Interesse an Staatssicherheit. Auch wenn moderne Ausspähungstechnologien eine Reaktion auf die komplexe internationale Bedrohungslage darstellen und aus sicherheitspolitischer Sicht als effektives Mittel zur Herstellung einer sicheren Welt gelten mögen, so bleibt dennoch die juristische Frage nach der Legalität dieser Maßnahmen. Der universelle Schutz der Menschenrechte lässt sich auch in diesem sensiblen Bereich, der immerhin der Sicherheit aller Menschen dient, nicht ausblenden. Die These „Der Zweck heiligt die Mittel" gilt in der juristischen Argumentation nämlich nicht bedingungslos. Auch wenn der Zweck einer Maßnahme von großer Bedeutung ist, muss das Mittel mit menschenrechtlichen Grundsätzen und Grenzen kompatibel sein. Anderenfalls kann auch der wichtigste Zweck ein menschenrechtswidriges Mittel nicht heiligen. Nachfolgend wird in diesem Sinne nach einer Darstellung des Schutzes der Privatsphäre in den Art. 17 IPbpR und Art. 8 EMRK die Vereinbarkeit von geheimdienstlicher Telekommunikationsüberwachung mit dem in diesen Artikeln niedergelegten Menschenrecht auf Privatsphäre untersucht.

Grundkonstellation dieses Abschnitts ist indes die geheimdienstliche Überwachung der Telekommunikation von Individuen innerhalb des Staatsgebiets.

A. Das internationale Menschenrecht auf Schutz der Privatsphäre

I. Der Schutz der Privatsphäre auf UN-Ebene

Nach einer Übersicht über geltende Bestimmungen und Bestrebungen zur Regulierung des Datenschutzes auf UN-Ebene wird das Menschenrecht auf Privatsphäre in Art. 17 IPbpR dargestellt.

1. Datenschutzbestimmungen auf UN-Ebene

Die rasante Entwicklung der Informations- und Kommunikationstechnologie im Laufe der letzten Jahrzehnte hat auf nationaler und internationaler Ebene die Frage nach dem rechtlichen Umgang mit den hiermit verbundenen neuen Herausforderungen ausgelöst. Der Datenschutz ist allmählich Gegenstand der nationalen Rechtsordnungen geworden.[146] Auch auf internationaler Rechtsebene wurden angesichts dieser technologischen Entwicklungen schon früh erste wegweisende Dokumente zum Datenschutz geschaffen. Die von der OECD im Jahre 1980 erlassenen Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten[147] sowie die vom Europarat 1981 verabschiedete Datenschutzkonvention[148] sind erste Vorstöße zur internationalen Verankerung des Datenschutzes.

Auch die UN befasste sich im Zuge der technologischen Entwicklungen schon früh mit Fragen des Datenschutzes. Bereits 1968 wurde die Frage nach den Auswirkungen des technologischen Fortschritts auf die Menschenrechte im Rahmen der internationalen Menschenrechtskonferenz in Teheran erstmals in einem breiten

[146] Unabhängig vom technologischen Wandel hat in Deutschland beispielsweise das Bundesverfassungsgericht mit dem Volkszählungsurteil von 1983 (BVerfGE 65, 1) den rechtlichen Grundstein für das Datenschutzrecht in Deutschland gelegt und grundlegende Datenschutzprinzipien entwickelt. Siehe dazu *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, S. 36 f. Vgl. auch *Bygrave*, Data Privacy Law, S. 99 f.

[147] Vgl. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23. September 1980, abrufbar unter www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [zuletzt abgerufen 01.12.2021]. Die 1980 verabschiedete Richtlinie wurde im Jahr 2013 überarbeitet und aktualisiert, vgl. http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [zuletzt abgerufen 01.12.2021].

[148] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28. Januar 1981, ETS No.108, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 [zuletzt abgerufen 01.12.2021]. Zur Europäischen Datenschutzkonvention und zur Novellierung der Konvention siehe 2. Abschnitt, Unterabschnitt A. II. 1.

internationalen Kontext erörtert.[149] Im Rahmen dieser Konferenz, die einen ersten Impuls für die internationale Auseinandersetzung mit Fragen des Datenschutzes auslöste, wurde letztlich die Empfehlung an die UN gerichtet, eine Studie über die Probleme der technologischen Entwicklungen für die Menschenrechte durchzuführen:

> „The organizations of the United Nations family should undertake a study of the problems with respect to human rights arising from developments in science and technology, particularly with regard to: (a) Respect for privacy in view of recording techniques; (b) Protection of the human personality and its physical and intellectual integrity in view of the progress in biology, medicine and biochemistry; (c) The uses of electronics which may affect the rights of the person and the limits which should be placed on its uses in a democratic society; (d) More generally, the balance which should be established between scientific and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity." [150]

Die Generalversammlung der UN hat im selben Jahr die erste Resolution zu der Frage nach den Gefahren der technologischen Entwicklungen für die Menschenrechte und konkret für die Privatsphäre erlassen.[151] Die in der Folge von UN-Sonderorganisationen und der Menschenrechtskommission zu diesem Thema erlassenen Berichte führten anschließend den durch die Teheraner Menschenrechtskonferenz in Gang gesetzten Prozess fort.[152] Die Generalversammlung hat am 14.12.1990 schließlich die „*Guidelines for the Regulation of Computerized Personal Data Files*" mit der Resolution 45/95 verabschiedet.[153] Resolutionen der UN-Generalversammlung sind nach Art. 10 der UN-Charta rechtlich unverbindlich. So haben auch die UN-

---

[149] Final Act of the International Conference on Human Rights: Teheran, A/CONF.32/41, 22. April – 13. Mai 1968, abrufbar unter http://daccess-ods.un.org/access.nsf/get?open&DS=A/CONF.32/41&Lang=E [zuletzt abgerufen 01.12.2021]; Vgl. dazu auch *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 118 ff.

[150] Final Act of the International Conference on Human Rights: Teheran, A/CONF.32/41, 22. April–13. Mai 1968, S. 12, abrufbar unter http://daccess-ods.un.org/access.nsf/get?open&DS=A/CONF.32/41&Lang=E [zuletzt abgerufen 01.12.2021].

[151] UN-Generalversammlung, Resolution 2450 (XXIII) Human rights and scientific and technological developments, 19. Dezember 1968, abrufbar unter https://undocs.org/pdf?symbol=en/A/RES/2450(XXIII) [zuletzt abgerufen 02.12.2021].

[152] Vgl. Wirtschafts- und Sozialrat der UN, Study of the Relevant Guidelines in the Field of Computerized Personnel Files, E/CN.4/Sub.2/1983/18, 30. Juni 1983, abrufbar unter http://daccess-ods.un.org/access.nsf/get?open&DS=E/CN.4/SUB.2/1983/18&Lang=E [zuletzt abgerufen 02.12.2021]. Siehe dazu *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 120 m.w.N.

[153] UN-Generalversammlung, Guidelines for the Regulation of Computerized Personal Data Files, A/RES/45/95, 14. Dezember 1990, abrufbar unter https://www.refworld.org/docid/3ddcafaac.html [zuletzt abgerufen 02.12.2021]. Im Folgenden: UN-Richtlinien zum Datenschutz.

Richtlinien zum Datenschutz, die sich an die Mitgliedstaaten der UN richten, folglich nur empfehlenden Charakter. Datenschutzrechtliche Mindestgarantien und Prinzipien werden in diesem Dokument definiert und dienen in diesem Sinne den Mitgliedstaaten als Orientierung, die diese Prinzipien in Form von nationalen Datenschutzgesetzen umsetzen sollten.

In dem im Vordergrund stehenden ersten Abschnitt werden datenschutzrechtliche Mindestgarantien definiert. Das Dokument beginnt im ersten Paragraphen mit der allgemeinen Klausel der Rechtmäßigkeit und Fairness („*Principle of lawfulness and fairness*"), wonach jede Sammlung und Verarbeitung personenbezogener Informationen nicht ungesetzlich und unfair erfolgen sowie die Nutzung nicht den Zielen und Prinzipien der UN-Charta entgegenstehen darf. Das Prinzip der Datenqualität („*Principle of accuracy*"), das die Gewährung und Kontrolle der Richtigkeit, Vollständigkeit und Relevanz der Daten zum Gegenstand hat, ist in § 2 der Richtlinien verankert. Des Weiteren dürfen nach § 3 Daten nur für zuvor definierte und legitime Zwecke erhoben werden („*Principle of purpose-specification*"). Die Datenerhebung ist nach der Erfüllung des bestimmten Zwecks zu beenden. Nach § 4 haben betroffene Personen das Recht zu erfahren, welche Daten über sie erhoben und gespeichert wurden („*Principle of interested-person access*"). Sofern die personenbezogenen Daten fehlerhaft sind oder auf unrechtmäßige Weise erlangt wurden, steht den betroffenen Personen das Recht zu, Korrektur oder Löschung der Daten zu verlangen. Das in § 7 niedergelegte Prinzip der Datensicherheit („*Principle of Security*") besagt, dass Daten etwa vor unbefugten Zugriffen, Verlust oder Verfälschung durch angemessene Maßnahmen gesichert werden müssen.

Mit den aufgelisteten Prinzipien der Rechtmäßigkeit, Zweckbindung, Datenqualität, Datensicherheit, Transparenz und das Auskunftsrecht für betroffene Individuen sind nahezu alle datenschutzrechtlichen Prinzipien, die die Grundpfeiler des heutigen Datenschutzstandards bilden und in zahlreichen nationalen Datenschutzgesetzen vorzufinden sind, verankert. Ein weiteres Grundprinzip des Datenschutzes ist das Prinzip der Datensparsamkeit, wonach möglichst wenige Daten erhoben werden sollen und die Verarbeitung und Speicherung über eine begrenzte Frist nicht hinausgehen darf.[154]

[154] Zu den datenschutzrechtlichen Grundprinzipien siehe *Bygrave*, Data Privacy Law, S. 145 ff. Die datenschutzrechtlichen Grundprinzipien sind beispielsweise in § 47 des deutschen Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) und im britischen Data Protection Act 2018 (Part 3, Chapter 2), abrufbar unter http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [zuletzt abgerufen 02.12.2021], vorzufinden. Siehe auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 28: „There is a growing global consensus on minimum standards that should govern the processing of personal data by States, business enterprises and other private actors. International instruments and guidelines reflecting this development include the 1990 Guidelines for the Regulation of Computerized Personal Data Files; the Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its modernized version [...]; the 1980 Organization for Economic Cooperation and Development Privacy Guidelines,

Dieses Dokument ist somit das erste wichtige Ergebnis der Bestrebungen auf Ebene der UN, eine globale Kultur des Datenschutzes zu schaffen. Dabei ist dieser Prozess noch lange nicht abgeschlossen. Denn die stetige Fortentwicklung der modernen Informations- und Telekommunikationstechnologie ist mit neuen, globalen Herausforderungen verbunden, die eine kontinuierliche Anpassung der internationalen Datenschutzkultur erforderlich machen kann. So haben etwa die *Snowden*-Enthüllungen unverkennbar gezeigt, dass auch heute noch – zwei Jahrzehnte nach Verabschiedung der UN-Richtlinien – der effektive Datenschutz auf globaler Ebene ein aktuelles und brisantes Thema bleibt. Am 18. Dezember 2013 hat die Generalversammlung der UN in der Resolution 68/167 hierauf Bezug genommen und folgendes festgestellt:[155]

> „The rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy […] and is therefore an issue of increasing concern".

In dieser Resolution betont die UN-Generalversammlung einerseits die Bedeutsamkeit des Schutzes der Privatsphäre sowie speziell des Datenschutzes und weist zudem auf die negativen Auswirkungen staatlicher Überwachungsmaßnahmen auf das Menschenrecht auf Privatsphäre hin. Die Generalversammlung fordert die Staaten auf, einerseits ihre nationalen Gesetze zu überprüfen, anzupassen sowie erforderliche Maßnahmen zu ergreifen, um den Schutz personenbezogener Daten als Ausprägung des Rechts auf Privatsphäre vor unberechtigter Überwachung effektiv zu schützen. Dabei wird auf die menschenrechtlichen Verpflichtungen aus dem IPbpR Bezug genommen. Das UN-Hochkommissariat für Menschenrechte (OHCHR) hat 2014 und zuletzt 2018 Berichte zum Thema „*The right to privacy in the digital age*" auf Anregung der UN-Generalversammlung angefertigt.[156] Diese Berichte heben den besonderen Stellenwert des Schutzes der Privatsphäre als Menschenrecht hervor und untersuchen in diesem Sinne die Konformität von geheimdienstlichen Überwachungsmaßnahmen mit Art. 17 IPbpR. Anwendungsbereich, Schutzumfang und Grenzen des Art. 17 IPbpR werden hier im konkreten Kontext von Überwachungs-

updated in 2013; the 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention); the Madrid resolution of the International Conference of Data Protection and Privacy Commissioners; and the 2015 Asia-Pacific Economic Coordination Privacy Framework, among others."

[155] UN-Generalversammlung, Resolution A/RES/68/167, 18.Dezember 2013.

[156] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014. Darüber hinaus hat der OHCHR im August 2018 erneut einen Bericht zu diesem Thema erlassen: Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018.

maßnahmen herausgearbeitet.[157] Damit ist der Bericht zweifelsfrei eine wichtige und wertvolle Quelle für die Auslegung des Schutzes der Privatsphäre in Art. 17 IPbpR.[158]

2. Der Schutz der Privatsphäre im IPbpR

Bereits in der Allgemeinen Erklärung der Menschenrechte (AEMR), mit deren Verabschiedung die UN-Generalversammlung im Jahr 1948 den Grundstein für den internationalen Menschenrechtsschutz gelegt hat,[159] wurde der Schutz der Privatsphäre als universelles Menschenrecht in Art. 12 niedergelegt. Die AEMR ist jedoch rechtlich unverbindlich. Erst mit der Verabschiedung des Internationalen Paktes über bürgerliche und politische Rechte am 16. Dezember 1966 durch die UN-Generalversammlung[160] wurde ein völkerrechtlicher Vertrag geschaffen, der den internationalen Schutz universeller Menschenrechte verbindlich kodifiziert hat. In Anlehnung an Art. 12 AEMR, ist der Schutz der Privatsphäre in Art. 17 IPbpR mit nahezu wortgleicher Formulierung statuiert. Am 23. März 1976 und somit zehn Jahre nach der Verabschiedung ist der IPbpR in Kraft getreten, nachdem 35 Staaten den Pakt ratifiziert hatten. Gemeinsam mit dem IPbpR ist auch das erste Fakultativprotokoll zum Individualbeschwerderecht angenommen worden und in Kraft getreten. Heute hat der IPbpR 173 Vertragsstaaten,[161] das erste Fakultativprotokoll hat 116 Mitgliedstaaten[162].

a. Der Menschenrechtsausschuss als Überwachungsorgan des IPbpR

Die Vertragsstaaten des IPbpR sind im Sinne des Art. 2 Abs. 1 des Paktes dazu verpflichtet, die im Pakt kodifizierten Menschenrechte zu achten und zu gewährleisten.[163] Des Weiteren müssen die Staaten gemäß Art 2 Abs. 3 IPbpR sicherstellen,

---

[157] Zum Schutzumfang des Art. 17 IPbpR siehe nachfolgenden Unterabschnitt A. I. 2. b.–d.

[158] So auch *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 143. Ein weiterer Schritt der UN zum Schutz der Privatsphäre und insbesondere der personenbezogenen Daten auf globaler Ebene war die Aufstellung eines Sonderberichterstatters für das Recht auf Privatsphäre, die mit der Resolution A/HRC/RES/28/16 im Jahr 2015 erfolgt ist. Der UN-Menschenrechtsrat ernannte Prof. Joseph Cannataci (Malta) als ersten Sonderberichterstatter für das Recht auf Privatsphäre, siehe dazu https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx [zuletzt abgerufen 02.12.2021].

[159] *Nowak*, CCPR Commentary, Introduction, S. XX, Rn. 2.

[160] UN-Generalversammlung, Resolution 2200 A (XXI), 16. Dezember 1966, A/6316 (1967), S. 49. Die Generalversammlung verabschiedete neben dem IPbpR zeitgleich auch den IPwskR. Diese beiden Pakte und die Fakultativprotokolle bilden gemeinsam mit der Allgemeinen Erklärung der Menschenrechte AEMR die sog. „International Bill of Human Rights“, siehe *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 68.

[161] Der aktuelle Stand der Mitgliedstaaten des IPbpR kann auf den Seiten der UN Treaty Collection eingesehen werden: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en [zuletzt abgerufen 22.02.2020].

[162] Vgl. UN Treaty Collection: https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND [zuletzt abgerufen 02.12.2021].

[163] Vgl auch *Nowak*, CCPR Commentary, Introduction, S. XXV, Rn. 14.

dass bei Verletzungen der im Pakt niedergelegten Rechte den betroffenen Individuen effektive Rechtsmittel zur Verfügung stehen. Die konkrete Implementierung des IPbpR in das nationale Rechtssystem und die nationale Durchsetzung der verankerten Rechte obliegt den Vertragsstaaten.[164] Mit der Unterzeichnung des Paktes haben die Staaten aber anerkannt, dass der UN-Menschenrechtsausschuss[165] (*Human Rights Committee*) im Sinne der Art. 28 ff. IPbpR als ständiges Vertragsorgan errichtet wird und die Einhaltung der Paktbestimmungen überwacht. So sind die Vertragsstaaten im Rahmen des obligatorischen Staatenberichtsverfahrens gemäß Art. 40 I IPbpR verpflichtet, dem Ausschuss regelmäßig Berichte über die Umsetzung ihrer Vertragsverpflichtungen vorzulegen. In diesen Berichten werden die innerstaatlichen Maßnahmen zur Durchsetzung der im Pakt statuierten Verpflichtungen und die auf diesem Weg bereits erzielten Fortschritte vorgestellt. Der Menschenrechtsausschuss prüft während der turnusmäßig stattfindenden Plenarsitzungen die Staatenberichte kritisch und stellt das Resultat seiner Prüfung in abschließenden Bemerkungen – den sogenannten *Concluding Observations* – zusammen.[166]

Die Mitgliedstaaten, die sich zudem unter dem ersten Fakultativprotokoll verpflichtet haben, unterliegen einem weiteren Kontrollverfahren. So gewährt Art. 1 des ersten Fakultativprotokolls Individuen, die sich unter der Jurisdiktion der betreffenden Staaten befinden, die Möglichkeit, dem Ausschuss Individualbeschwerden („*Communications*") über Menschenrechtsverletzungen durch den Vertragsstaat vorzulegen. Nach der Prüfung der Beschwerde teilt der Menschenrechtsausschuss gemäß Art. 5 Abs. 4 S. 1 des Fakultativprotokolls seine Ansichten über die Beschwerde („*Views*") dem Individuum und dem Staat mit.[167]

Die *General Comments* sind allgemeine Bemerkungen des Menschenrechtsausschusses zu bestimmten Themen oder einzelnen Paktbestimmungen, die sich an alle Vertragsstaaten richten. In den *General Comments* fasst der Menschenrechtsausschuss seine Interpretationen der kodifizierten Menschenrechte zusammen.[168] Auf diese Weise werden dem naturgemäß weiten Wortlaut der Menschenrechte konkrete Konturen verliehen sowie gleichsam die Vertragspflichten der Staaten spezifiziert.

Im Wege dieser Trias – *Concluding Observations*, *Views* und *General Comments* – legt der Menschenrechtsausschuss mithin die im IPbpR statuierten Menschenrechte aus und ruft die Staaten dazu auf, die Paktbestimmungen seinen Auslegungen entsprechend zu berücksichtigen. Die Zahl der eingehenden Individualbeschwerden ist jedoch – insbesondere im Vergleich zum Europäischen Gerichtshof für Menschen-

---

[164] *Nowak*, CCPR Commentary, Introduction, S. XXV, Rn. 15.
[165] Im Folgenden „MRA".
[166] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.37, 1.40; *Buergenthal,* The U.N. Human Rights Committee, in von Bogdandy/Wolfrum (Hrsg.), Max Planck Yearbook of United Nations Law, S. 350.
[167] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.48 ff. Neben dem Individualbeschwerdeverfahren sieht Art. 41 IPbpR ein Staatenbeschwerdeverfahren vor, das allerdings die freiwillige Unterwerfung der jeweiligen Staaten voraussetzt.
[168] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.44.

rechte – verhältnismäßig gering.[169] Infolgedessen können aus dem entsprechend limitierten Bestand an *Views*, in denen der Ausschuss freilich nur auf die fallspezifischen Rechtsfragen eingeht, nicht immer ausführliche Interpretationen zu allen Menschenrechtsfragen gewonnen werden. Vor diesem Hintergrund sind die *Concluding Observations*, die regelmäßig die Staatenberichtsverfahren abschließen, eine wertvolle Erkenntnisquelle für die Auslegung des IPbpR durch den Menschenrechtsausschuss. Zwar formuliert der Ausschuss die *Concluding Observations* im Kontext bestimmter Staatenberichte, jedoch sind diese Aussagen und Empfehlungen Ausdruck einer grundsätzlichen Interpretation des Paktes. Die jeweils berichterstattenden Staaten sind direkte Adressaten der entsprechenden *Concluding Observations*, allerdings spiegeln sich darin indirekt prinzipielle und allgemeine Ansichten und Interpretationen des Ausschusses wider.[170] Dies zeigt sich insbesondere auch daran, dass der Menschenrechtsausschuss in den letzten Jahren in seinen *General Comments* auf *Concluding Observations* verwiesen und damit diese Empfehlungen als Quelle allgemeiner Interpretationen herangezogen hat.[171]

Die Entscheidungen und Stellungsnahmen des Menschenrechtsausschusses haben indes keine rechtliche Bindungswirkung, da der Ausschuss kein Gericht im eigentlichen Sinne ist, sondern vielmehr als quasi-juristisches Organ agiert.[172] Die *Views* sowie die *Concluding Observations* und *General Comments* sind letztlich für die Mitgliedstaaten nicht verbindlich.[173] Dennoch haben die Entscheidungen und Stellungnahmen des Ausschusses großes Gewicht.[174] So spielt der Menschenrechtsausschuss, der eigens durch den Vertrag zur Interpretation und Überwachung des Paktes errichtet wurde, für die Auslegung des IPbpR eine zentrale Rolle.[175] Der Inter-

---

[169] Im gesamten Zeitraum von 1977 bis März 2017 sind insgesamt 2.970 Beschwerden beim Menschenrechtsauschuss eingegangen, vgl. Report of the Human Rights Committee, 117th session (20 June–15 July 2016)/118th session (17 October–4 November 2016)/119th session (6–29 March 2017), A/72/40, Rn. 24. Im Gegensatz dazu wurden allein im Jahr 2018 43.100 Beschwerden beim Europäischen Gerichtshof für Menschenrechte eingereicht, vgl. Annual Report 2018 of the European Court of Human Rights, Council of Europe, S. 167, abrufbar unter https://www.echr.coe.int/Pages/home.aspx?p=court/annualreports&c [zuletzt abgerufen 02.12.2021].

[170] Vgl. *Buergenthal,* The U.N. Human Rights Committee, in von Bogdandy/Wolfrum (Hrsg.), Max Planck Yearbook of United Nations Law, S. 351

[171] Im *General Comment* zu Art. 9 IPbpR sind zahlreiche Verweise auf *Concluding Observations* zu finden (UN Human Rights Committee, General Comment No. 35: Article 9 (Liberty and security of person), CCPR/C/GC/35, 16. Dezember 2014). Vgl. auch UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of opinion and expression), CCPR/C/GC/34, 12. September 2011.

[172] Vgl. UN Human Rights Committee, General Comment No. 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights, CCPR/C/GC/33, 25. Juni 2009, Rn. 11; Siehe auch *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 261.

[173] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.60.

[174] Siehe auch *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 266 f., die von einer „erhöhten Legitimität" des Ausschusses sprechen.

[175] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.61.

nationale Gerichtshof[176] hat die bedeutende Funktion des Ausschusses in seinem Urteil im Fall *Diallo* zum Ausdruck gebracht.[177] Zudem hat der Menschenrechtsausschuss selbst im *General Comment* 33 erklärt, dass seine *Views* charakteristische Merkmale einer Gerichtsentscheidung aufweisen:

> „11. […] the views issued by the Committee under the Optional Protocol exhibit some important characteristics of a judicial decision. They are arrived at in a judicial spirit, including the impartiality and independence of Committee members, the considered interpretation of the language of the Covenant, and the determinative character of the decisions. […]
>
> 13. The views of the Committee under the Optional Protocol represent an authoritative determination by the organ established under the Covenant itself charged with the interpretation of that instrument. These views derive their character, and the importance which attaches to them, from the integral role of the Committee under both the Covenant and the Optional Protocol."[178]

Die Vertragsstaaten haben sich durch Unterzeichnung des Paktes gemäß dem Prinzip „*pacta sunt servanda*" verpflichtet, hinsichtlich des Vertrages und der Umsetzung ihrer Pflichten in gutem Glauben zu handeln.[179] Diese Verpflichtung erstreckt sich ebenso auf die Kooperation mit dem Vertragsorgan:

---

[176] Im Folgenden „IGH".

[177] International Court of Justice, Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo), Merits, Judgment, I.C.J. Reports 2010, S. 639, Rn. 66. Dies kommt auch im sogenannten Mauergutachten des IGH zum Ausdruck: International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136, Rn. 109 f.

[178] UN Human Rights Committee, General Comment No. 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights, CCPR/C/GC/33, 25. Juni 2009, Rn. 13 und 15.

[179] So heißt es im UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 3: „Pursuant to the principle articulated in article 26 of the Vienna Convention on the Law of Treaties, States Parties are required to give effect to the obligations under the Covenant in good faith." Vgl. auch *Buergenthal,* The U.N. Human Rights Committee, in von Bogdandy/ Wolfrum (Hrsg.), Max Planck Yearbook of United Nations Law, S. 397: „As States parties to the Covenant, these states have also undertaken to give effect to Covenant rights on the domestic plane and to provide an effective remedy for their violation. A Committee determination that a state has violated a right guaranteed in the Covenant therefore enjoys a normative and institutional legitimacy that carries with it a justifiable expectation of compliance."

> „A duty to cooperate with the Committee arises from an application of the principle of good faith to the observance of all treaty obligations.“[180]

Zudem haben die Unterzeichnerstaaten des Fakultativprotokolls dem Ausschuss die Befugnis erteilt, Individualbeschwerden zu prüfen und über das Vorliegen von Menschenrechtsverletzungen zu entscheiden.[181] Demnach ist eine Nichtbefolgung der Entscheidungen des Menschenrechtsausschuss ein starkes Indiz dafür, dass ein Staat seine Verpflichtungen aus dem IPbpR missachtet.[182] Darüber hinaus geraten die Staaten durch die Nichtbefolgung der Entscheidungen in den Blickpunkt der internationalen Gemeinschaft und stehen im Sinne des Prinzips „*naming and shaming*“ unter internationalem Druck.[183] Trotz mangelnder rechtlicher Bindungswirkung der Entscheidungen des Ausschusses und fehlender Durchsetzungsmechanismen für die Vertragspflichten, hat die Spruchpraxis des Menschenrechtsausschuss somit dennoch gewichtigen Einfluss in den Vertragsstaaten und leistet damit einen bedeutenden Beitrag für die Umsetzung der Paktbestimmungen.

b. Schutzumfang des Art. 17 IPbpR

Das Menschenrecht auf Schutz der Privatsphäre wurde mit der Verabschiedung des IPbpR im Artikel 17 verbindlich kodifiziert. Dass die Formulierung des Artikels 17 IPbpR in Anlehnung an Artikel 12 AEMR erfolgte, ist zweifelsfrei an dem fast identischen Wortlaut beider Normen zu erkennen.[184]

> „Article 17
>
> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.“

Artikel 17 IPbpR kodifiziert den Schutz der Privatsphäre als Abwehrrecht und Schutzpflicht. Diese Ansicht hat sich während der Entstehungsphase des Paktes

[180] UN Human Rights Committee, General Comment No. 33: The Obligations of States Parties under the Optional Protocol to the International Covenant on Civil and Political Rights, CCPR/C/GC/33, 25. Juni 2009, Rn. 15.
[181] *Buergenthal,* The U.N. Human Rights Committee, in von Bogdandy/Wolfrum (Hrsg.), Max Planck Yearbook of United Nations Law, S. 397.
[182] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 1.61.
[183] Ebd.
[184] Die Formulierung des Art. 12 AEMR lautet: „No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.“

durchgesetzt[185] und wird in der Praxis des Menschenrechtsausschusses so interpretiert.[186] So hat der Ausschuss im *General Comment* 16 hierzu ausgeführt:

> „In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[187]

Hier wird einerseits der aus Artikel 17 IPbpR hervorgehende Schutz vor staatlichen Beeinträchtigungen und andrerseits die Verpflichtung der Staaten, Individuen vor Beeinträchtigungen durch natürliche und juristische Personen zu schützen, zum Ausdruck gebracht. Artikel 17 Abs. 2 IPbpR garantiert ausdrücklich den Anspruch auf rechtlichen Schutz gegen Beeinträchtigungen.[188]

Neben dem allgemeinen Schutz des Privaten („*privacy*") umfasst Art. 17 IPbpR ausdrücklich auch den Schutz spezieller Ausprägungen der Privatsphäre, nämlich die Familie („*family*"), die Wohnung („*home*"), die Korrespondenz („*correpondence*") sowie die Ehre und den Ruf („*honour and reputation*"). Dabei bieten diese weiten Begriffe einen breiten Interpretationsspielraum, sodass die unterschiedlichen Erscheinungsformen dieser Schutzgüter und die kulturellen Diversitäten in den Mitgliedstaaten erfasst werden können.[189] Beispielsweise hat sich der Menschenrechtsausschuss im *General Comment* 16 für eine weite Interpretation des Begriffs „Familie" ausgesprochen, sodass unterschiedliche kulturelle Auffassungen über den Familienkreis grundsätzlich erfasst werden.[190]

Bedeutsam ist insbesondere die weite Auslegung von „*privacy*". Der Begriff „*privacy*" dient als Auffangtatbestand und schützt die Tatbestände der Privatsphäre, die

---

[185] *Nowak*, CCPR Commentary, Art. 17, S. 379 f, Rn. 6. Einige Staaten (u.a. die USA, Großbritannien und Australien) plädierten für eine ausschließliche Abwehrfunktion, da anderenfalls Änderungen in den Zivilrechtsordnungen notwendig würden. Weder die Menschenrechtskommission noch die Generalversammlung folgten indes dieser Ansicht. Vgl. *Bossuyt,* Guide to the „Travaux Préparatoires", S. 341.

[186] Die Schutzpflichten der Mitgliedstaaten aus Art. 17 IPbpR sind unten im 3. Abschnitt, Unterabschnitt B. I. 3. a. ausführlich dargestellt.

[187] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, abrufbar unter: http://www.refworld.org/docid/453883f922.html [zuletzt abgerufen 02.12.2021].

[188] Siehe dazu *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 16.15.

[189] *Nowak*, CCPR Commentary, S. 393, Art.17, Rn. 31; *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 83f.

[190] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 5. Gleichermaßen wird der Begriff „Wohnung" weit interpretiert und umfasst nach der Auslegung des Ausschusses etwa auch den Arbeitsplatz.

nicht von den in Art. 17 IPbpR benannten speziellen Ausprägungen umfasst sind.[191] Dabei bietet dieser offene Begriff unfraglich einen besonders weiten Interpretationsspielraum, den der Menschenrechtsausschuss in seiner bisherigen Spruchpraxis genutzt hat, um weitere wichtige Bereiche der Privatsphäre in den Schutzkreis des Artikels 17 IPbpR einzuschließen. Auf dieser Grundlage hat der Ausschuss etwa das Recht am eigenen Namen[192], die sexuelle Selbstbestimmung[193] sowie den Schutz personenbezogener Daten[194] aus „*privacy*" abgeleitet.

c. Der Schutz der Korrespondenz in Art. 17 IPbpR

Zum Zeitpunkt der Verabschiedung des Paktes im Jahr 1966 bezog sich der Begriff „*correspondence*" hauptsächlich auf den brieflichen Schriftverkehr.[195] Der weite Begriff „*correspondence*" setzt allerdings keine unüberwindbaren begrifflichen Grenzen für eine weitergehende Auslegung, die die Entwicklungen der Telekommunikationstechnologie berücksichtigt. So hat der Menschenrechtsausschuss im Wege der dynamischen Auslegung den Begriff der Korrespondenz auf alle heutigen Formen der Telekommunikation ausgedehnt, sodass beispielsweise Telefonie, Telefax, Emailverkehr sowie sonstige Formen elektronischer sowie internetgestützter Kommunikation umfasst sind.[196] Auch moderne Formen des persönlichen Informationsaustausches auf öffentlichen Plattformen und in Social Media wie *Facebook* oder *Instagram* werden grundsätzlich als „Korrespondenz" unter Art. 17 geschützt.[197]

Art. 17 IPbpR schützt die Vertraulichkeit und Diskretion der Korrespondenz.[198] Im *General Comment* 16 wird dazu ausgeführt:

[191] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 95.
[192] *Coeriel and Aurik v. The Netherlands,* No. 453/1991, CCPR/C/52/D/453/1991, 9. Dezember 1994.
[193] UN Human Rights Committee, *Toonen v. Australia*, No. 488/1992, CCPR/C/50/D/488/1992, 31. März 1994, Rn. 8.2.
[194] Siehe dazu 2. Abschnitt, Unterabschnitt A. I. 2. d.
[195] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 90.
[196] Vgl. UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 8: „Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited". Siehe auch *Nowak*, CCPR Commentary, Art. 17, S. 401, Rn. 47.
[197] Siehe dazu *Seibert-Fohr,* Digital Surveillance, Meta Data and Foreign Intelligence Cooperation, S. 3.
[198] *Nowak*, CCPR Commentary, Art. 17, S. 401, Rn. 47; *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 16.32.

> „Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read.“[199]

Dieser in Artikel 17 IPbpR niedergelegte Schutz ist Ausdruck eines menschlichen Grundbedürfnisses und empfindlichen Bereichs der individuellen Privatsphäre. So sind der interpersonelle Dialog und Austausch von Informationen, Gedanken oder Emotionen für Menschen, die als soziale Wesen in organisierten Gesellschaften leben und in Sozialgemeinschaften alltäglich agieren, unentbehrlich. Die freie individuelle Entscheidung über den Adressatenkreis, den Inhalt und der Form der Kommunikation sowie die Respektierung der Vertraulichkeit ist für die Realisierung dieses Grundbedürfnisses von essentieller Bedeutung.

In diesem Sinne konstituiert Artikel 17 IPbpR die Verpflichtung für Staaten, die Vertraulichkeit der Korrespondenz zu schützen. Wie der Ausschuss im zitierten *General Comment* ausführt, schützt Art. 17 IPbpR die ungestörte und ausspähungsfreie Übertragung der Korrespondenz. Der Schutzumfang dieses Menschenrechts erstreckt sich damit auf die Geheimhaltung und die Privatheit der Korrespondenz.[200] Unabhängig davon, welche konkreten Inhalte mittels der gewählten Korrespondenzform zwischen Absender und Empfänger ausgetauscht werden, muss gemäß Art. 17 IPbpR die ungestörte Übertragung der Nachrichten gewährleistet werden. Der menschenrechtliche Schutz der Vertraulichkeit der Korrespondenz erstreckt sich darüber hinaus auch auf die Verkehrsdaten der Telekommunikation,[201] wie etwa Daten über Korrespondenzbeteiligte, Zeit, Ort oder Dauer der Korrespondenz.[202] Demnach muss auch die Vertraulichkeit dieser Metadaten gewahrt werden. Die Verkehrsdaten dürfen mithin nicht während der Übermittlung beispielsweise eingesehen oder abgefangen werden. Die Metadaten geben zwar keinen Aufschluss über die ausgetauschten Inhalte. Jedoch können sie durchaus sensible persönliche Informationen preisgeben sowie – bei systematischer Sammlung solcher Daten – persönliche Verhaltensmuster oder beispielsweise soziale Beziehungen offenlegen.[203] Damit sind sie gerade für polizeiliche oder geheimdienstliche Ermittlungsarbeiten von großer Bedeutung. Zudem sind sie auch aus technischer Sicht untrennbare Bestandteile der geschützten Telekommunikation.[204]

---

[199] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 8.

[200] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 16.32.

[201] So auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 19. Außerdem *Seibert-Fohr,* Digital Surveillance, Meta Data and Foreign Intelligence Cooperation, S. 3 m.w.N.

[202] Siehe dazu 1. Abschnitt, Unterabschnitte A. I.

[203] Siehe auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 19.

[204] Siehe oben 1. Abschnitt Unterabschnitt A. I.

Die Staaten müssen einerseits im Rahmen ihrer abwehrrechtlichen Verpflichtung aus Art. 17 IPbpR Eingriffe in die Vertraulichkeit der Korrespondenz unterlassen. Beispiele für Eingriffe in die Vertraulichkeit der Korrespondenz sind typischerweise die heimliche Ausspähung und Aufzeichnung von Telekommunikation sowie die Nicht-Übermittlung, Zensur oder Veröffentlichung von privater Korrespondenz.[205] Solche Eingriffe können unter den in Art. 17 IPbpR bestimmten Voraussetzungen und Grenzen im Einzelfall gerechtfertigt sein.[206]

Zudem sind die Staaten nach Absatz 2 verpflichtet, durch gesetzliche Regelungen und andere Maßnahmen sicherzustellen, dass Eingriffe von privaten Akteuren untersagt werden. Damit trägt Artikel 17 Abs. 2 IPbpR etwa dem Umstand Rechnung, dass Telekommunikations-Dienstleistungen nicht ausschließlich von staatlicher Hand angeboten werden, sondern auch private Dienstleister als Anbieter auftreten.[207] Insofern muss auch im Rahmen von Korrespondenz-Übertragungsdiensten in privater Hand sichergestellt werden, dass die menschenrechtlich geschützte Vertraulichkeit der Korrespondenz gewährleistet wird. Hinsichtlich der Ausgestaltung solcher gesetzlichen Regelungen und Maßnahmen haben die Staaten einen weiten Entscheidungsspielraum.[208]

In der Spruchpraxis des Menschenrechtsausschusses zum Schutz der Korrespondenz wurden bisher vornehmlich Fälle der Korrespondenzüberwachung von Strafgefangenen entschieden.[209] Mit dem Thema der Telekommunikationsüberwachung hat sich der Ausschuss in der Entscheidung *Antonius Cornelis Van Hulst v. The Netherlands* befasst.[210] Dieser Fall betraf die Abhörung und Aufzeichnung der Telefonkorrespondenzen zwischen dem Beschwerdeführer und seinem Anwalt.

d. Der Datenschutz in Art. 17 IPbpR

Der Schutz von personenbezogenen Daten wird in Artikel 17 IPbpR nicht ausdrücklich genannt. Der Menschenrechtsausschuss hat aber früh die mit dem technologischen Wandel einhergehenden Gefahren für den Schutz von persönlichen Daten erkannt und dementsprechend Art. 17 IPbpR dynamisch ausgelegt. So wird der Datenschutz aus dem allgemeinen Auffangtatbestand „*privacy*" abgeleitet.[211] Das

---

[205] *Nowak*, CCPR Commentary, Art. 17, S. 401, Rn. 48.

[206] Zu den Voraussetzungen für die Rechtfertigung von Eingriffen in die Vertraulichkeit der Korrespondenz, siehe 2. Abschnitt Unterabschnitt B. II.

[207] *Nowak*, CCPR Commentary, Art. 17, S. 401, Rn. 47.

[208] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 91. Zum Umfang der Schutzpflichten aus Art. 17 IPbpR siehe unten 3. Abschnitt, Unterabschnitt B. I. 3. a.

[209] UN Human Rights Committee, *Larry James Pinkney v. Canada,* No. 27/1978, CCPR/C/OP/1 at 12 (HRC 1980), 29. Oktober 1981; *Angel Estrella v. Uruguay*, No. 74/1980, CCPR/C/18/D/74/1980, 29. März 1983; *Boodoo v. Trinidad and Tobago*, No. 721/1996, CCPR/C/74/D/721/1996, 02. April 2002; *Daniel Pinto v. Trinidad and Tobago,* No. 512/1992, CCPR/C/57/D/512/1992, 24. Juni 1994; *Crafton Tomlin v. Jamaica,* No. 589/1994, CCPR/C/57/D/589/1994, 16. Juli 1996.

[210] UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004.

[211] *Nowak*, CCPR Commentary, Art. 17, S. 388, Rn. 23.

Recht auf Datenschutz ist eine besondere Ausprägung der Privatsphäre unter Art. 17 IPbpR. Schutzgegenstand des Datenschutzes ist die Geheimheit und Vertraulichkeit personenbezogener Daten.[212] Dieser Schutz erstreckt sich im Rahmen von Telekommunikationsdaten auch auf die Metadaten der Korrespondenz.[213] Gemäß Art. 17 Abs. 1 IPbpR steht jedem Individuum das Recht zu, selbst über die Preisgabe und Verarbeitung seiner personenbezogenen Daten zu bestimmen. Jede staatliche Handlung zur Erhebung, Sammlung, Veröffentlichung und sonstiger Verarbeitung von personenbezogenen Informationen, die ohne oder entgegen dem Willen des Datensubjekts geschieht, stellt einen Eingriff in den Schutzbereich des Art. 17 IPbpR dar. Dieses aus Art. 17 IPbpR hervorgehende Recht auf informationelle Selbstbestimmung hat der Menschenrechtsausschuss im Jahr 1988 mit der Erarbeitung des *General Comment* 16 konkretisiert:

> „The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."[214]

Gemäß Art. 17 Abs. 2 IPbpR sind die Staaten verpflichtet, durch effektive datenschutzrechtliche Regulierungen personenbezogene Daten vor unberechtigten staatlichen oder privaten Eingriffen zu schützen.[215]

Im zitierten *General Comment* werden in diesem Sinne datenschutzrechtliche Prinzipien aufgezählt, die die Staaten in ihren nationalen Gesetzen inkorporieren sollen. Zugleich hat der Menschenrechtsausschuss im Rahmen der regelmäßigen Staatenberichtsverfahren einzelner Mitgliedstaaten des Paktes auf die nationale Umsetzung dieser Verpflichtung hingewiesen. Dabei hat der Ausschuss nicht nur auf

---

[212] Ebd. Rn. 21 ff.

[213] Siehe dazu bereits oben 2. Abschnitt, Unterabschnitt A. I. 2. c.

[214] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 10.

[215] *Nowak*, CCPR Commentary, Art. 17, S. 388, Rn. 23; *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 82.

die im *General Comment* ausdrücklich genannten Prinzipien Bezug genommen. Vielmehr wird anhand von *Concluding Observations* unterschiedlicher Staatenberichtsverfahren deutlich, dass der Ausschuss die Prinzipien im Laufe der vergangenen Jahre nach Annahme des *General Comment* 16 konkretisiert und wesentlich weiterentwickelt hat. All diese Prinzipien, die nach Auslegung des Menschenrechtsausschusses aus Art. 17 IPbpR abzuleiten sind, spiegeln einige der heute anerkannten internationalen Grundprinzipien des Datenschutzes wider.[216]

So beginnt der zitierte Auszug aus dem *General Comment* 16 mit dem Prinzip der Rechtmäßigkeit. Jede Erhebung und Speicherung von personenbezogenen Daten muss gesetzlich geregelt sein.[217] Der Menschenrechtsausschuss hat in einigen *Concluding Observations* neuester Zeit dazu angemerkt, dass die Gesetze hinreichend bestimmt und präzise sowie öffentlich zugänglich sein müssen.[218] Des Weiteren muss der Zweck der Datenerhebung und -speicherung bestimmt[219] und zudem mit dem Pakt und den hierin statuierten Verpflichtungen der Staaten vereinbar sein.[220] Durch wirkungsvolle Maßnahmen müssen die Staaten ferner sicherstellen, dass nur die durch das zugrundeliegende Gesetz zum Umgang mit den Daten ausdrücklich berechtigten Personen Zugang zu den Daten haben.[221] Die nationalen Datenschutzgesetze müssen darüber hinaus den betroffenen Individuen das Recht einräumen, in verständlicher Form über die Art der gespeicherten persönlichen Daten und den Zweck der Speicherung informiert zu werden. Darüber hinaus müssen die Individuen dazu berechtigt sein, die Berichtigung oder Löschung von Daten zu verlangen,

[216] Die Datenschutzprinzipien sind im Rahmen der Datenschutzrichtlinie dargestellt worden, siehe 2. Abschnitt, Unterabschnitt A. I. 1.

[217] Siehe auch UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/4, 31. Juli 2008, Rn. 22.

[218] Siehe etwa UN Human Rights Committee, Concluding observations: United States of America, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22; UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12.

[219] Der Menschenrechtsausschuss hat das Prinzip der Zweckbindung und -bestimmung in den Concluding observations für Großbritannien hinsichtlich der Sammlung von Kommunikationsdaten erwähnt: „The State party should: […] (b) Ensure that any interference with the right to privacy, with the family, with the home or with correspondence is authorized by laws that […] (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims." UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; Vgl. auch UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12.

[220] Vgl. UN Human Rights Committee, Concluding observations: Sweden, CCPR/C/SWE/CO/6, 7. Mai 2009, Rn. 18: „The State party should take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant, and be consistent with obligations under article 17 of the Covenant."

[221] Das Prinzip der Datensicherheit ist auch in den Concluding observations für Frankreich zu finden, siehe UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/4, 31. Juli 2008, Rn. 22.

die entweder unrichtig sind oder unter Missachtung der gesetzlichen Vorschriften erlangt oder bearbeitet wurden. Hierin manifestieren sich sowohl der Grundsatz der Transparenz, das Recht auf Einflussnahme der betroffenen Individuen sowie das Prinzip der Datenqualität.[222] Der Menschenrechtsausschuss hat diese wichtigen Prinzipien auch im *General Comment* 34, das sich mit dem in Art 19 IPbpR statuierten Menschenrecht auf Meinungs- und Informationsfreiheit befasst, eingefügt[223]:

> „Elements of the right of access to information are also addressed elsewhere in the Covenant. As the Committee observed in its general comment No. 16, regarding article 17 of the Covenant, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control his or her files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to have his or her records rectified."

Im *General Comment* 16 klingt an anderer Stelle außerdem das grundlegende Prinzip der Datensparsamkeit an, wonach nur so viele Daten erhoben und gespeichert werden dürfen, die für die Erreichung des legitimen Zwecks erforderlich sind:

> „As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant."[224]

[222] Vgl. auch UN Human Rights Committee, Concluding observations: Republic of Korea, CCPR/C/79/Add. 114, 1. November 1999, Rn. 17; UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/4, 31. Juli 2008, Rn. 22: „Taking into account general comment No. 16 (1988) on Article 17 (Right to privacy), the State party should in particular ensure that […] (c) Individuals under its jurisdiction have the right to request rectification or elimination of information when it is incorrect or has been collected or processed contrary to the provisions of the law". Siehe außerdem *Bygrave*, Data Privacy Law, S. 85.

[223] UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of opinion and expression), CCPR/C/GC/34, 12. September 2011, Rn. 18.

[224] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 7. Vgl. andererseits aber auch die Concluding Observations für Ungarn, in denen der MRA das hohe Maß an Datenschutz und den Mangel an verfügbaren Daten zur Evaluierung der Menschenrechtssituation in dem Staat kritisiert, UN Human Rights Committee, Concluding observations: Hungary, CCPR/C/HUN/CO/5, 16. November 2010, Rn. 6:

Der Menschenrechtsausschuss hat sich überdies bisher eher kritisch hinsichtlich der Vorratsdatenspeicherung geäußert.[225] Auch das ist ein Beleg dafür, dass der Ausschuss eine Begrenzung der Datenerhebung und Speicherung auf das notwendige Maß im Sinne der Datensparsamkeit aus dem Schutz der personenbezogenen Daten in Artikel 17 IPbpR ableitet. Besonders deutlich ist diese Auslegung des Ausschusses in den *Concluding Observations* für Großbritannien zu erkennen:

> „The State party should: […] (d) Revise the Data Retention and Investigatory Powers Act 2014 with a view to ensuring that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes and is dependent upon prior judicial authorization“.[226]

Seit 2014 hat der Menschenrechtsausschuss in einer Reihe von *Concluding Observations* hervorgehoben, dass „any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity“.[227] Dieser Appell wurde bislang stets im Kontext von staatlichen Überwachungsmaßnahmen ausgesprochen, die die Vertraulichkeit privater Korrespondenz und den Schutz personenbezogener Daten tangieren. Neben dem Prinzip der Rechtmäßigkeit („*legality*“) und dem Prinzip der Datensparsamkeit sowie Erforderlichkeit („*necessity*“) wird

---

„The Committee is concerned at the high level of protection afforded by Act LXIII of 1992 [...], which prohibits the collection of disaggregated personal data of any kind. The Committee is concerned that this prohibition impedes it from effectively monitoring the implementation of the provisions of the Covenant. (arts. 2 and 17)
The State party should review the [...] to ensure that it is in line with the Covenant, particularly article 17, as expounded by the Committee in its general comment No. 16. The State party should ensure that the protection afforded to personal data should not hinder the legitimate collection of data that would facilitate the monitoring and evaluation of programmes that have a bearing on the implementation of the Covenant.“

[225] Siehe etwa UN Human Rights Committee, Concluding observations: South Africa, CCPR/C/ZAF/CO/1, 27. April 2016, Rn. 42; UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; UN Human Rights Committee, Concluding observations: United States of America, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22; Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 29 f.

[226] UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24 [Hervorh. d. Verf.]. Ein ähnliche Formulierung ist auch in den Concluding observations für Estland vorzufinden: UN Human Rights Committee, Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 29 f.

[227] UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12. Siehe zudem UN Human Rights Committee, Concluding observations: United States of America, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22; Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; Concluding observations: South Africa, CCPR/C/ZAF/CO/1, 27. April 2016, Rn. 42; Concluding observations: Sweden, CCPR/C/SWE/CO/7, 28. April 2016, Rn. 37; Concluding observations: Norway, CCPR/C/NOR/CO/7, 25. April 2018, Rn. 21; Concluding observations: Equatorial Guinea, CCPR/C/GNQ/CO/1, 22. August 2019, Rn. 51.

hier insbesondere auch die Verhältnismäßigkeit („*proportionality*") als wichtiges Kriterium für die Rechtfertigung von Engriffen in den Datenschutz genannt.

Schließlich wird im eingangs zitierten Auszug des *General Comment* 16 auch das Bestehen unabhängiger Kontrollbehörden erwähnt. In diesem Zusammenhang wird auch in einigen *Concluding Observations* das Erfordernis genannt, unabhängige Aufsichtsbehörden einzurichten, die die vorschriftsmäßige Erhebung, Speicherung und Nutzung der persönlichen Daten überwachen sollen.[228]

Diese Zusammenstellung verdeutlicht, dass der Menschenrechtsausschuss im *General Comment* 16 wichtige Grundlagen des modernen Datenschutzes aus Art. 17 IPbpR ableitet und im Laufe seiner Spruchpraxis den Schutz personenbezogener Daten weiter konkretisiert hat. Eine Neufassung des *General Comment* 16 würde den aktuellen Stand der Auslegung des Art. 17 IPbpR des Ausschusses in Hinblick auf den Datenschutz zusammentragen und sicherlich weitere Details einbeziehen. Dies wäre durchaus zu begrüßen, aber keineswegs zwingend notwendig.

II. Der Schutz der Privatsphäre in der EMRK

1. Die Datenschutzkonvention des Europarates

Am 28.01.1981 hat der Europarat mit der Verabschiedung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[229] das erste verbindliche internationale Datenschutzabkommen geschaffen.[230] Zweck des Übereinkommens ist die Substantiierung und Konkretisierung des Datenschutzes als spezielle Ausprägung des in Art. 8 EMRK verankerten Schutzes der Privatsphäre. Zudem dient die Konvention einer Regulierung des

[228] So heißt es in den Concluding observations des Staatenberichtsverfahrens von Schweden (2009): „To that effect, the State party should guarantee that the processing and gathering of information be subject to review and supervision by an independent body with the necessary guarantees of impartiality and effectiveness." UN Human Rights Committee, Concluding observations: Sweden, CCPR/C/SWE/CO/6, 7. Mai 2009, Rn. 18. Siehe außerdem UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; UN Human Rights Committee, Concluding observations: Sweden, CCPR/C/SWE/CO/7, 28. April 2016, Rn. 37.

[229] Im Folgenden: „europäische Datenschutzkonvention". Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, 28 January 1981, abrufbar unter: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [zuletzt abgerufen 02.12.2021]. Die englische und französische Version sind verbindlich. Ein im Jahr 2001 erlassenes Zusatzprotokoll beinhaltet konkretere Regeln zur transnationalen Datenübermittlung sowie zur Errichtung von nationalen Datenschutzstellen, die den Vollzug der Datenschutzkonvention überwachen sollen. Die Regulierungen im Zusatzprotokoll wurden im Zuge der aktuellen Novellierung der Konvention in den Konventionstext implementiert. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No. 181, 8 November 2001, abrufbar unter: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181 [zuletzt abgerufen 02.12.2021]. Zur Novellierung siehe unten.

[230] *Bygrave*, Data Privacy Law, S. 31.

grenzüberschreitenden Datentransfers sowie einer Harmonisierung der Datenschutzstandards in den einzelnen Mitgliedstaaten, um den Weg für einen grenzüberschreitenden Datenverkehr zu ebnen.[231]

Die europäische Datenschutzkonvention wurde bislang von den 47 Mitgliedstaaten des Europarates unterzeichnet und ratifiziert. Zudem können Nichtmitgliedstaaten des Europarates gemäß Art. 23 der Konvention vom Ministerkomitee eingeladen werden, der Datenschutzkonvention beizutreten. So haben beispielsweise auch Uruguay, Mauritius und Senegal nach entsprechender Einladung die Datenschutzkonvention unterzeichnet und ratifiziert. Insgesamt sind bis dato 55 Staaten Vertragsparteien des Übereinkommens.[232]

Im März 2010 hat das Ministerkomitee des Europarates eine Novellierung der Datenschutzkonvention beschlossen, um das nun über 35 Jahre alte Dokument an die Entwicklungen der modernen Technologien anzupassen.[233] Überdies strebt der Europarat mit der Modernisierung eine Harmonisierung der Konvention mit dem Datenschutzrecht der EU – insbesondere mit der Datenschutz-Grundverordnung[234] – an.[235]

In einem internationalen Konsultationsverfahren sind Stellungnahmen und Vorschläge von Regierungen und privaten Organisationen für die Modernisierung geprüft und ausgewertet worden.[236] Das eigens hierfür eingesetzte Ad-Hoc Komitee für Datenschutz (CAHDATA) hat im Juni 2016 schließlich den konsolidierten Entwurf für die modernisierte Fassung der europäischen Datenschutzkonvention

[231] Die Motive und Ziele der europäischen Datenschutzkonvention gehen aus der Präambel deutlich hervor: „The member States of the Council of Europe […] Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;[…] Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".

[232] Die Liste der Mitgliedstaaten der europäischen Datenschutzkonvention ist abrufbar unter: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=N55z0zVf [zuletzt abgerufen 02.12.2021].

[233] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 318f.

[234] Europäische Union, Verordnung 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) – EU Amtsblatt v. 4.5.2016, L119/1.

[235] Siehe dazu die Erklärungen des Europarates über den Prozess und den Zweck der Novellierung auf der eigenen Webseite: http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet [zuletzt abgerufen 02.12.2021].

[236] Bis Mai 2011 sind 50 Stellungnahmen eingegangen. Zusammenstellung über die Stellungnahmen im Rahmen des Konsultationsverfahrens: Bureau of the Consultative Committee of the Convention 108, „Consultation concerning the modernisation of Convention 108: results" (T-PD-BUR(2011) 01 MOS rev 6), June 2011, abrufbar unter: http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af2ef [zuletzt abgerufen 02.12.2021].

abgeschlossen.[237] Im Mai 2018 hat das Ministerkomitee das Änderungsprotokoll verabschiedet.[238] Im Februar 2020 haben bereits 35 Staaten das Änderungsprotokoll unterzeichnet.[239] Die konsolidierte Fassung ist zwar noch nicht in Kraft. Die folgenden Ausführungen basieren dennoch auf der novellierten Fassung der Datenschutzkonvention.

Die europäische Datenschutzkonvention wird völkerrechtlich verbindlich sein. Gemäß Art. 4 sind die Vertragsparteien dazu verpflichtet, in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen zu treffen, um die in der Konvention aufgestellten Grundsätze für den Datenschutz zu verwirklichen. Die modernisierte Fassung hebt dabei hervor, dass neben der gesetzlichen Kodifizierung der datenschutzrechtlichen Grundsätze auch die effektive Umsetzung von den Staaten gewährleistet werden müsse. Dies geht aus der Änderung des Wortlauts des Art. 4 Abs. 1 hervor. Des Weiteren beruht auch die Neufassung des Art. 4 Abs. 3 auf diesen Grundgedanken. So wird hier ein verbindlicher Prozess zur Evaluierung der Effektivität von Maßnahmen, die von den Staaten zur Umsetzung ihrer Verpflichtungen aus der Konvention durchgeführt werden, festgesetzt.[240]

Anwendungsbereich und Gegenstand der Konvention ist der Schutz des Rechts auf Privatsphäre[241] bei der Verarbeitung von personenbezogenen Daten (Art. 1)[242], wobei die Regelungen der Konvention auf den öffentlichen und privaten Bereich Anwendung finden (Art. 3 Abs.1). Die Vertragsparteien haben nach Art. 11 zudem die Möglichkeit, ein über den in der Konvention kodifizierten Mindeststandard hinausgehendes Schutzniveau zu gewähren.

Das Herzstück der Datenschutzkonvention ist das Kapitel II, das die allgemeinen Grundsätze des Datenschutzes verankert.[243] Art. 5 umfasst dabei mehrere

---

[237] Das Ad-Hoc Komitee (offizielle Bezeichnung: Ad hoc Committee on Data protection CAHDATA) wurde unter Art. 17 der Satzung des Europarates eingesetzt und ist für die Modernisierung der Europäischen Datenschutzkonvention zuständig. Die endgültige konsolidierte Version des Entwurfs für die Modernisierung der europäischen Datenschutzkonvention (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data) von Mai 2018 ist abrufbar unter: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf [zuletzt abgerufen 02.12.2021].

[238] https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108 [zuletzt abgerufen: 02.012.2021].

[239] Siehe offizielle Liste der Unterzeichnungen, abrufbar unter https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures [zuletzt abgerufen 02.12.2021].

[240] Das Konventionskomitee im Sinne des 7. Kapitels der Konvention ist gemäß Art. 4 Abs. 3 für die Durchführung dieses Evaluierungsprozesses zuständig.

[241] Die in der englischen Version vorzufindende Bezeichnung „*right to privacy*“ wird in der deutschen Übersetzung der Konvention als „Recht auf einen Persönlichkeitsbereich“ bezeichnet. Für die vorliegende Arbeit wird der Bezeichnung „Recht auf Privatsphäre“ aus Gründen der Einheitlichkeit Vorzug gegeben.

[242] Während im Originaldokument von 1981 die *automatisierte* Verarbeitung (*automatic prosessing*) von Daten Regelungsgegenstand der Konvention war, weitet die modernisierte Fassung den Anwendungsbereich auf jegliche Verarbeitungen (*data prossesing*) aus. Siehe dazu die Legaldefinitionen in Art. 2 lit. b und c der novellierten Konvention.

[243] Siehe auch *Bygrave*, Data Privacy Law, S. 36 f.

Kernprinzipien des Datenschutzes. In der aktualisierten Fassung ist das Prinzip der Verhältnismäßigkeit nunmehr an erster Stelle im Art. 5 Abs. 1 niedergelegt. Weiterhin werden neben dem Grundprinzip der Rechtmäßigkeit (Art. 5 Abs. 3) außerdem die Prinzipien der Transparenz sowie der Zweckbestimmung und -bindung genannt (Art. 5 Abs. 4 lit. a, b). Das Prinzip der Transparenz ist zudem in Art. 8 der novellierten Fassung ausführlich niedergelegt. Des Weiteren wird im Sinne des Prinzips der Datensparsamkeit verlangt, dass gesammelte Daten nicht länger gespeichert werden dürfen, als für den festgelegten Zweck erforderlich ist (Art. 5 Abs. 4 lit. c, e). Schließlich müssten die Daten sachlich richtig und gegebenenfalls auf den neuesten Stand sein (Art. 5 Abs. 4 lit. d), womit das Prinzip der Datenqualität zum Ausdruck gebracht wird. Datensicherheit ist in Art. 7 reguliert, wonach geeignete Sicherungsmaßnahmen gegen unbefugten Zugang, Veränderung, Zerstörung oder unbefugtes Bekanntgeben getroffen werden müssen. Ein besonderer Schutzmaßstab gilt für sensible Daten, wie beispielsweise Daten über die Gesundheit, über etwaige Vorstrafen oder das Sexualleben einer Person. Solche Daten dürfen gemäß Art. 6 nur verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet.

Art. 9 der novellierten Datenschutzkonvention reguliert die Rechte betroffener Individuen. Beispielsweise müssen Betroffene auf Verlangen regelmäßig in verständlicher Form Information über die Verarbeitung von ihren personenbezogenen Daten erhalten (Art. 9 Abs. 1 lit. b). Außerdem legt Art. 9 Abs. 1 lit. e etwa einen Korrektur- und Löschungsanspruch nieder, sofern personenbezogene Daten entgegen der datenschutzrechtlichen Grundsätze nach Art. 5 und 6 verarbeitet wurden. Gemäß Art. 9 Abs. 1 lit. d steht dem Betroffenen auch das grundsätzliche Recht zum Widerspruch gegen die Datenverarbeitung zu.

Kapitel III reguliert den grenzüberschreitenden Datenverkehr zwischen den Vertragsparteien untereinander sowie mit Nicht-Vertragsparteien des Übereinkommens. In Art. 14 Abs. 2 der novellierten Fassung wird festgelegt, dass der Datenverkehr mit Nicht-Mitgliedern möglich ist, wenn dieser Staat oder diese Organisation ein angemessenes Schutzniveau für die beabsichtigte Datenweitergabe gewährleistet. Die näheren Voraussetzungen sind in den folgenden Absätzen reguliert.

Während die Ursprungsfassung der Datenschutzkonvention keine Vorschrift zur Errichtung von staatlichen Aufsichtsbehörden für Datenschutz enthielt[244] und erst durch Art. 1 des Zusatzprotokolls von 2001 dieser wichtige Themenbereich reguliert wurde,[245] widmet sich das Kapitel IV in der Novellierung allein diesem Thema. So schreibt Art 15 die Errichtung von nationalen Aufsichtsbehörden vor und reguliert ausführlich deren Aufgabenbereich und Kompetenzen.

Insgesamt wird deutlich, dass die novellierte Europäische Datenschutzkonvention die heute anerkannten Kernprinzipien des Datenschutzes umfassend niederlegt. Zur Zeit ihres Inkrafttretens war die Konvention ein sehr fortschrittliches und

[244] Vgl. *Bygrave*, Data Privacy Law, S. 39, der dies als „Lücke" in der Konvention bezeichnet.
[245] Zum Zusatzprotokoll von 2001 siehe Fn 229.

wegweisendes Dokument. In Reaktion auf die technologischen Entwicklungen im letzten Viertel des zwanzigsten Jahrhunderts und das Aufkeimen eines neuen IT-Zeitalters ist es dem Europarat gelungen, zentrale Grundprinzipien des Datenschutzes zu definieren und im Rahmen eines verbindlichen Übereinkommens als Mindeststandard zu kodifizieren. Die Novellierung der Konvention holt nun die technologischen Entwicklungen der vergangenen 35 Jahre auf.

2. Der Schutz der Privatsphäre in Art. 8 EMRK

Die Europäische Menschenrechtskonvention ist am 04.11.1950 in Rom vom Europarat verabschiedet worden und etwa drei Jahre später am 3.9.1953, nachdem 10 Staaten die Konvention ratifiziert hatten, als verbindlicher völkerrechtlicher Vertrag in Kraft getreten.[246] Alle 47 Mitgliedstaaten des Europarates haben die EMRK ratifiziert.[247] Die in der Konvention garantierten Rechte können von Individuen aus den Vertragsstaaten im Wege der Individualbeschwerde (Art. 34 EMRK) beim Europäischen Gerichtshof für Menschenrechte (EGMR) direkt eingeklagt werden.[248] Die Urteile des EGMR sind für die betroffenen Staaten gemäß Art. 46 EMRK bindend. Seit Beginn der Arbeitsaufnahme in Straßburg ist die Zahl der jährlich eingehenden Individualbeschwerden beim EGMR beträchtlich.[249] Das Repertoire der Spruchpraxis bietet dementsprechend viele differenzierte Urteile zu den einzelnen Menschenrechten. So ist auch die Rechtsprechung zum Schutz der Privatsphäre gemäß Art. 8 EMRK umfangreich.[250]

---

[246] Council of Europe, Convention for the Protection Human Rights and Fundamental Freedoms, ETS No.005, 04 November 1950, abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 [zuletzt abgerufen 02.12.2021].

[247] Der aktuelle Ratifikationsstand der Menschenrechtskonvention ist abrufbar unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=iX4nf8MT [zuletzt abgerufen 02.12.2021].

[248] Bis Oktober 1998 wurden Beschwerden wegen einer Verletzung der EMRK oder eines seiner Zusatzprotokolle zunächst von der Europäischen Menschenrechtskommission (EKMR) geprüft, bevor sie an den Gerichtshof verwiesen wurden. Seit Oktober 1998 ist nun ausschließlich der ständige Europäische Gerichtshof für Menschenrechte zuständig. Für die Durchsetzung von dessen Urteilen ist das Ministerkomitee des Europarates zuständig (Art. 46 Abs. 2 EMRK). Neben den Individualbeschwerdeverfahren sieht die EMRK auch Staatenbeschwerden (Art. 33 EMRK) sowie Gutachtenverfahren (Art. 47 EMRK) vor, die in der Praxis allerdings eine eher untergeordnete Rolle spielen. Vgl. *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 165 f. m.w.N.

[249] Seit seiner Arbeitsaufnahme im Jahre 1959 bis 2018 hat der EGMR insgesamt über 841.300 Anträgen entschieden, siehe dazu Council of Europe, ECHR Overview 1959–2018 (März 2019), abrufbar unter https://www.echr.coe.int/Documents/Overview_19592018_ENG.pdf [zuletzt abgerufen 02.12.2021].

[250] *Mowbray*, European Convention on Human Rights, S. 488.

a. Der Schutzumfang des Art. 8 EMRK

Das Recht auf Achtung der Privatsphäre ist in Art. 8 EMRK verankert. Unter dem Titel „*Right to respect for private and family life*“ schützt Art. 8 Abs. 1 neben dem Privat- und Familienleben ausdrücklich auch die Wohnung und die Korrespondenz:

> „1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.“

Ebenso wie Art. 17 IPbpR, ist auch Art. 8 EMRK in Anlehnung und Orientierung an Art. 12 AEMR entstanden.[251] Allerdings wird der Schutz der Ehre und des guten Rufes im Gegensatz zu Art. 17 IPbpR nicht ausdrücklich in Art. 8 Abs. 1 EMRK genannt.[252] Das Familienleben, die Wohnung und die Korrespondenz sind besondere Ausprägungen des Privatlebens. Der Begriff „Privatleben“ („*private life*“) ist indes sehr weit und umfasst alle weiteren Bereiche der Privatsphäre, die nicht unter den ausdrücklich genannten Ausprägungen fallen. Dabei können sich die Schutzbereiche der einzelnen in Art. 8 RMRK genannten Ausprägungen in vielen Fällen auch überschneiden.[253] Die Kommission und der EGMR haben in ihrer Judikatur indes keine allgemeinen Abgrenzungskriterien entwickelt, sondern die Abgrenzung für jeden konkreten Einzelfall entschieden.[254]

Der EGMR hat die Begriffe „Familienleben“, „Wohnung“ und „Korrespondenz“ in seiner Spruchpraxis definiert und die Konturen des Schutzumfangs dieser Rechte dargelegt.[255] Im Gegensatz zu diesen konkreten und erfassbaren Begriffen, lässt sich aus dem offenen und weiten Begriff „Privatleben“ nicht ohne weiteres erschließen, wo die Grenzen des Schutzgehaltes dieses Rechts liegen. So hat auch

---

[251] So wurde in der Entstehungsphase der Konvention für Art 8 EMRK zunächst eine Formulierung vorgeschlagen, die dem Wortlaut von Art. 12 AEMR sehr ähnlich war, vgl. dazu *Frowein* in *Frowein/ Peukert*, EMRK-Kommentar, Art. 8, S. 288, Rn. 2. Die Formulierung des Art. 8 EMRK war in der Entstehungsphase Gegenstand vieler Diskussionen. Insbesondere bestand zunächst Uneinigkeit darüber, welche Ausprägungen der Privatsphäre – wie etwa der Schutz des Familienlebens – ausdrücklich aufgezählt werden sollten. Vgl. dazu *Schabas,* The European Convention on Human Rights, Art. 8, S.359 ff sowie *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 167 ff.

[252] Siehe dazu *Schabas,* The European Convention on Human Rights, Art. 8, S.362.

[253] *Siemen,* Datenschutz als europäisches Grundrecht, S. 53.

[254] Ebd., S. 54.

[255] Zum Begriff „Familienleben“ siehe EGMR, *Marckx v. Belgium*, Rs. 6833/74, 13. Juni 1979, Serie A31, Rn. 31; siehe außerdem zum Begriff „Wohnung“ beispielsweise EGMR, *Chappell v. The United Kingdom,* Rs. 10461/83, 30. März 1989, Serie A152-A, Rn. 26, 51.

der EGMR in seiner Spruchpraxis eindeutig zum Ausdruck gebracht, dass es nicht möglich und notwendig sei, eine umfassende und abschließende Definition von „*private life*" festzulegen.[256] Vielmehr erfasse dieser weite Begriff vielfältige Aspekte der physischen und sozialen Identität einer Person.[257] Im Laufe seiner Judikatur hat der Gerichtshof indes einige Rechte aus dem Schutz des Privatlebens abgeleitet. Der Schutz der physischen sowie psychischen Integrität von Personen[258], das Recht am eigenen Bild[259], das Recht auf sexuelle Identität[260] und der Schutz des guten Rufes[261] sind nur eine Auswahl der bislang aus dem „Privatleben" gemäß Art. 8 EMRK vom EGMR hergeleiteten Rechte. Auch der Schutz personenbezogener Daten wird hieraus abgeleitet.[262]

Der in Art. 8 EMRK verankerte Schutz der Privatsphäre ist in erster Linie als Abwehrrecht gegen staatliche Beeinträchtigungen ausgestaltet.[263] Darüber hinaus fließen aus Art. 8 EMRK aber auch Schutzpflichten, die die Konventionsstaaten zum Schutz der Privatsphäre vor Beeinträchtigungen durch Dritte verpflichten.[264]

b. Der Schutz der Korrespondenz in Art. 8 EMRK

Zum Zeitpunkt der Verabschiedung der EMRK umfasste der Begriff „*correspondence*" in erster Linie den klassischen schriftlichen Briefverkehr.[265] Ebenso wie der MRA, hat auch der EGMR auf Grundlage einer dynamischen Auslegung festgestellt, dass „Korrespondenz" im Zuge der Entwicklungen der Kommunikationstechnologie alle elektronischen und auch internetbasierten Formen der Telekommunikation umfasst.[266] Der Wortlaut des Art. 8 EMRK steht dieser dynamischen Auslegung nicht entgegen.[267] Damit sind neben Briefen auch Telefongespräche, Telefaxe, Emails[268] sowie Internettelefonie und andere internetgestützte Kommuni-

---

[256] EGMR, *Niemitz v. Germany,* Rs. 13710/88, 16. Dezember 1992, Serie A251-B, Rn. 29; *Pretty v. The United Kingdom,* Rs. 2346/02, 29. April 2002, Rep. 2002-III, Rn. 61; *Peck v. The United Kingdom,* Rs. 44647/98, 28. January 2003, Rep. 2003-I, Rn. 57.

[257] EGMR, *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 66.

[258] EGMR, *X and Y v. the Netherlands*, Rs. 8978/80, 26. März 1985, Serie A 91, Rn. 22; *Y.F. v. Turkey*, Rs. 24209/94, 22. Juli 2003, Rep. 2003-IX, Rn. 33.

[259] EGMR, *Von Hannover v. Germany*, Rs. 59320/00, 24. Juni 2004, Rep. 2004-VI, Rn. 103.

[260] EGMR, *Dudgeon v, The United Kingdom,* Rs. 7525/76, 22. Oktober 1981, Serie A45, Rn. 41; siehe außerdem *Hämäläinen v. Finland* [GC], Rs. 37359/09, 16. Juli 2014, Rep. 2014, Rn. 59.

[261] EGMR, *Chauvy and Others v. France*, Rs. 64915/01, 29. Juni 2004, Rep. 2004-VI, Rn. 70.

[262] Siehe nachfolgenden Unterabschnitt A. II. 2. c.

[263] EGMR, *P. and S. v. Poland*, Rs. 57375/08, 30. Oktober 2012, Rn. 94.

[264] *Schabas,* The European Convention on Human Rights, Art. 8, S.367 ff. Zum Umfang der Schutzpflichten aus Art. 8 EMRK im Allgemeinen und im konkreten Fall der extraterritorialen Telekommunikationsüberwachung siehe 3. Abschnitt, Unterabschnitt B. I.

[265] *Frowein* in *Frowein/Peukert*, EMRK-Kommentar, Art. 8, S. 314, Rn. 48.

[266] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 41; *Schabas,* The European Convention on Human Rights, Art. 8, S. 400 f.

[267] *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 221.

[268] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 118.

kationsformen als „Korrespondenz" unter Art. 8 Abs. 1 EMRK geschützt.[269] Der Schutz der Korrespondenz hat in der Spruchpraxis des EGMR einerseits hinsichtlich der Korrespondenzüberwachung von Strafgefangenen eine wichtige Rolle gespielt.[270] Allerdings hat sich der Gerichtshof bislang auch in einer Reihe von Fällen mit der Vereinbarkeit von Maßnahmen zur Telekommunikationsüberwachung mit dem Schutz der Korrespondenz befasst.[271]

Gegenstand des Schutzes ist auch im Rahmen von Art. 8 EMRK die Vertraulichkeit der Korrespondenz während des Übermittlungsprozesses vom Absenden bis zum Empfang der Nachricht.[272] Somit sind auch nur solche Mitteilungen geschützt, die für einen begrenzten Adressatenkreis – unter Ausschluss der Öffentlichkeit – bestimmt sind.[273] Dabei kommt es nicht darauf an, ob der Korrespondenztransfer durch staatliche oder private Stellen ausgeführt wird.[274] Des Weiteren sind sowohl private als auch geschäftliche Korrespondenzen geschützt.[275] Auch bereits empfangene und gespeicherte Nachrichten fallen unter den Schutz des Art. 8 Abs. 1 EMRK. Dies hat der EGMR schon im Fall *Niemitz v. Germany* entschieden und diese Rechtsprechung auch in jüngeren Fällen bestätigt.[276]

---

[269] EGMR, *Copland v. The United Kingdom*, Rs. 62617/00, 03. April 2007, Rep. 2007-I, Rn. 41. Internetgestützte Kommunikationsdienstleistungen sind beispielsweise *Skype* und *WhatsApp*. Siehe auch *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 219 f.

[270] EGMR, *Silver and Others v. The United Kingdom*, Rs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, 25. März 1983, Serie A 61; EGMR, *Golder v. The United Kingdom*, Rs. 4451/70, 21. Februar 1975, Serie A 18; EGMR, *De Wilde, Ooms and Versyp v. Belgium*, Rs. 2832/66, 2835/66, 2899/66, 18. November 1970, Serie A 12; EGMR, *Campbell and Fell* v. The United Kingdom, Rs. 7819/77, 7878/77, 28. Juni 1984, Serie A 80; EGMR, *Boyle and Rice v. The United Kingdom*, Rs. 9659/82, 9658/82, 27. April 1988, Serie A 131. Dies gilt ebenso für die Spruchpraxis des UN-Menschenrechtsausschuss, siehe 2. Abschnitt, Unterabschnitt A. I. 2.c.

[271] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28; EGMR, *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95; EGMR, *Kruslin v. France*, Rs. 11801/85, 24. April 1990, Serie A 176-A; EGMR, *Kopp v. Switzerland*, Rs. 23224/94, 25. März 1998, Rep. 1998-II; EGMR, *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008; *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021.

[272] EGMR, *Michaud v. France*, Rs. 12323/11, 6. Dezember 2012, Rn. 90; außerdem *Grabenwarter,* European Convention on Human Rights, Art.8, S. 198, Rn. 27 und 28.

[273] Das Kriterium des Ausschlusses der Öffentlichkeit kann hinsichtlich persönlicher Profile auf sozialen Netzwerken im Einzelfall schwierig zu beurteilen sein. Öffentliche Posts auf *Facebook* sind nicht an einen konkreten Adressatenkreis gerichtet und stellen infolgedessen keine Korrespondenz im Sinne des Art. 8 EMRK dar. Werden diese Posts indes nur mit einem definierten Freundeskreis des Profilinhabers geteilt, so ist die Öffentlichkeit mithin ausgeschlossen und der Schutzbereich des Art. 8 EMRK ist eröffnet. Vgl. *Paefgen,* Persönlichkeitsrechte im Internet, S. 14, 18.

[274] *Grabenwarter,* European Convention on Human Rights, Art.8, S. 198, Rn. 27.

[275] Im Fall *Niemitz v. Germany*, Rs. 13710/88, 16. Dezember 1992, Rn. 32 hat der EGMR die Vereinbarkeit der Durchsuchung einer Anwaltskanzlei mit Art. 8 EMRK geprüft und dabei u.a. deutlich zum Ausdruck gebracht, dass sich der Schutz der Korrespondenz keinesfalls nur auf den privaten Bereich erstreckt.

[276] Vgl. *Grabenwarter,* European Convention on Human Rights, Art.8, S. 198, Rn. 27; EGMR, *Niemitz v. Germany*, Rs. 13710/88, 16. Dezember 1992, Serie A251-B, Rn. 32. Im Fall *Wieser and Bicos*

Nach Rechtsprechung des EGMR sind zudem auch Telekommunikations-Verbindungsdaten vom Schutz der Korrespondenz nach Art. 8 EMRK erfasst.[277] Nachdem der Gerichtshof in der Entscheidung *Malone v. The United Kingdom*[278] dies erstmals für Telefon-Metadaten feststellte, hat er dies in der Entscheidung *Copland v. The United Kingdom* für jegliche Form der Korrespondenz bestätigt:

> „The Court observes that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an ‚integral element of the communications made by telephone' (see Malone v. the United Kingdom […]). […] the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8."[279]

Damit erstreckt sich der Schutz der Korrespondenz nicht nur auf die Vertraulichkeit des Inhaltes, sondern auch auf die Vertraulichkeit der Informationen über Zeit, Ort, Häufigkeit, Adressat und auf sonstige Metadaten der Korrespondenz.

c. Der Datenschutz in Art. 8 EMRK

Der Datenschutz wird in Art. 8 EMRK zwar nicht ausdrücklich genannt. Der EGMR legt den allgemeinen Schutz des Privatlebens („*private life*") gemäß Art. 8 Abs. 1 EMRK jedoch weit aus und leitet hieraus auch den Schutz von personen-

---

Beteiligungen GmbH v. Austria, Rs. 74336/01, 16. Oktober 2007, Rep. 2007-IV wurden Daten – einschließlich Korrespondenzdaten mit Mandanten – auf dem Computer einer Anwaltskanzlei beschlagnahmt. Der EGMR stellte einen Eingriff in das Recht auf Achtung der Korrespondenz fest. Vgl. auch *Bernh Larsen Holding A S and Others v. Norway*, Rs. 24117/08, 14. März 2013.

[277] Siehe dazu bereits hinsichtlich Art. 17 IPbpR 2. Abschnitt, Unterabschnitt A. I. 2. c.

[278] EGMR, *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 84: „The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)."

[279] EGMR, *Copland v. The United Kingdom*, Rs. 62617/00, 03. April 2007, Rep. 2007-I, Rn. 43–44.

bezogenen Daten ab.[280] In diesem Zusammenhang verweist der Gerichtshof in einigen Urteilen auf die Europäische Datenschutzkonvention.[281]

Gegenstand des Datenschutzes ist auch unter Art. 8 EMRK die Vertraulichkeit und Geheimheit von personenbezogenen Daten.[282] In seiner Judikatur hat der EGMR den Schutzumfang und die aus Art. 8 EMRK hervorgehenden datenschutzrechtlichen Ansprüche der Individuen umfassend definiert. Danach statuiert Art. 8 EMRK das Recht auf informationelle Selbstbestimmung, wonach jedem Individuum das Recht zusteht, über Preisgabe und Verwendung personenbezogener Daten grundsätzlich selbst zu bestimmen.[283] So steht dem Individuum einerseits das Recht zu, dem Staat personenbezogene Informationen nicht preiszugeben und dem Staat einen Zugang zu diesen Daten zu verwehren.[284] Befinden sich personenbezogene Daten hingegen bereits in der Hand des Staates, so gewährt Art. 8 EMRK dem Datensubjekt einen Schutz vor Verarbeitung – wie etwa Verwendung, Archivierung, Weitergabe oder Veröffentlichung – der Daten.[285]

Das Recht auf Datenschutz gemäß Art. 8 EMRK bezieht sich indes auf „personenbezogene" Daten. Der EGMR hat sich in seiner bisherigen Rechtsprechung mit der Auslegung dieses Begriffs eingehend befasst. Neben einer Darstellung dieser Spruchpraxis wird im Folgenden außerdem der Frage nachgegangen, inwieweit der Gerichtshof in seiner Judikatur auf die datenschutzrechtlichen Grundprinzipien der Europäischen Datenschutzkonvention Bezug nimmt.

---

[280] *Grabenwarter,* European Convention on Human Rights, Art.8, S.189, Rn. 10. Während sich die Kommission und der Gerichtshof in der frühen Judikatur zunächst eher zögerlich mit der Frage nach dem Schutz personenbezogener Daten unter Art. 8 EMRK befasst haben, wurde diese Frage im Laufe der Zeit in einer Reihe von Fällen relevant. Im Urteil *Z. v. Finland*, Rs. 22009/93, 25. Februar 1997, Rep. 1997-I, Rn. 95 hat der EGMR erstmals ausdrücklich die grundlegende Bedeutung des Datenschutzes für das Recht auf Achtung des Privatlebens betont: „In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention." Daraufhin hat der Datenschutz Einzug in die Rechtsprechung des EGMR gefunden. Zur Entwicklung der Rechtsprechung des EGMR und der Kommission zum Datenschutz siehe *Siemen,* Datenschutz als europäisches Grundrecht, S. 79 ff.

[281] EGMR, *P.G. and J.H. v. The United Kingdom*, Rs. 44787/98, 25. September 2001, Rep. 2001-IX, Rn. 57; EGMR, *Rotaru v. Romania* [GC], Rs. 28341/95, 4. Mai 2000, Rep. 2000-V, Rn. 43; EGMR, *Cemalettin Canli v. Turkey*, Rs. 22427/04, 18. November 2008, Rn. 34; EGMR, *Amann v. Switzerland* [GC], Rs. 27798/95, 16. Februar 2000, Rep. 2000-II, Rn. 65; EGMR, *Uzun v Germany*, Rs. 35623/05, 2. September 2010, Rn. 46.

[282] Vgl. *Schabas,* The European Convention on Human Rights, Art. 8, S. 382.

[283] So hat der EGMR in einigen Fällen in der Erhebung von personenbezogenen Daten einen Eingriff festgestellt. So etwa in Fällen der Abhörung von Telefonaten, vgl. EGMR *Halford v. The United Kingdom*, Rs. 20605/92, 25. Juni 1997, Rep. 1997-III. In anderen Fällen hingegen stellte die Verarbeitung der Daten einen Eingriff in Art. 8 EMRK dar, wie beispielsweise die Veröffentlichung der Daten im Fall *Peck v. The United Kingdom*, Rs. 44647/98, 28. January 2003, Rep. 2003-I. Vgl. auch *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 96 ff.

[284] Ebd., S. 81 ff.

[285] *Grabenwarter,* European Convention on Human Rights, Art.8, S.189, Rn. 10.

aa. Der Begriff „Personenbezogene Daten" in der Rechtsprechung des EGMR

Der Gerichtshof verweist in seiner Judikatur auf die in Art. 2 der Europäischen Datenschutzkonvention niedergelegte Definition des Begriffs „personenbezogene Daten" („*personal data*"). So heißt es etwa in der Entscheidung *Amann v. Switzerland*:

> „[The Court] points out in this connection that the term ‚private life' must not be interpreted restrictively. […] That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, [...] whose purpose is ‚to secure in the territory of each Party for every individual [...] his right to privacy, with regard to automatic processing of personal data relating to him' (Article 1), such personal data being defined as ‚any information relating to an identified or identifiable individual' (Article 2)."[286]

Der Gerichtshof legt diese Begriffsbestimmung für Art. 8 EMRK zugrunde.[287] Danach sind „personenbezogene Daten" jegliche Informationen über eine bestimmte oder bestimmbare natürliche Person.[288] Es muss folglich eine Verknüpfung zwischen der Information und einer konkreten Person bestehen, wobei diese Person zumindest identifizierbar sein muss.

Der Name und die Abbildung einer Person sind Kernaspekte der persönlichen Identität und insofern zweifelsfrei als personenbezogene Daten zu qualifizieren.[289] Hinsichtlich der Aufzeichnung einer Stimmprobe (sog. „*Voice Sample*") zum Zwecke der Identifizierung einer Person im Zuge von polizeilichen Ermittlungen hat der Gerichtshof im Fall *P.G. and J.H. v. The United Kingdom* das Vorliegen personenbezogener Daten angenommen.[290] Auch DNA-Profile, Zellproben und Fingerabdrücke wurden vom EGMR als personenbezogene Daten qualifiziert.[291] Dabei hat

---

[286] EGMR, *Amann v. Switzerland* [GC], Rs. 27798/95, 16. Februar 2000, Rep. 2000-II, Rn. 65.

[287] Siehe auch EGMR, *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 68: „The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals."
Der EGMR entscheidet grundsätzlich nicht über Verletzungen der Europäischen Datenschutzkonvention (zur Europäischen Datenschutzkonvention siehe 2. Abschnitt, Unterabschnitt A. II.1.). Dies geht im Umkehrschluss aus Art. 19 EMRK hervor, wonach der Gerichtshof die Einhaltung der Verpflichtungen aus der EMRK durch die Vertragsstaaten sicherstellt. Das schließt jedoch nicht aus, dass der EGMR bei seinen Urteilen die Datenschutzkonvention ergänzend heranziehen kann.

[288] Siehe auch die allgemeine Begriffsbestimmung oben 1. Abschnitt, Unterabschnitt A. I.

[289] Siehe EGMR, *Khmel v. Russia*, Rs. 20383/04, 12. Dezember 2013, Rn. 40 m.w.N.

[290] EGMR, *P.G. and J.H. v. The United Kingdom*, Rs. 44787/98, 25. September 2001, Rep. 2001-IX, Rn. 59.

[291] EGMR, *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 68.

der Gerichtshof im Fall *S. and Marper v. The United Kingdom* hervorgehoben, dass Zellproben zahlreiche sensible Informationen etwa über die Gesundheit und Genetik einer Person enthalten.[292] Für die Beurteilung der datenschutzrechtlichen Legitimität der Speicherung von Zellproben kommt es dem EGMR zufolge nicht darauf an, inwieweit der Datenverarbeiter zum Zeitpunkt der Speicherung die Möglichkeit hat, auf alle inkludierten Informationen zuzugreifen. Vielmehr ist auf dem objektiven Informationsgehalt der Zellproben abzustellen, auch wenn diese erst durch zukünftige Technologien dekodiert und somit nachvollziehbar gemacht werden können.[293] Diesen objektivierten Ansatz führt der Gerichtshof auch im Zusammenhang mit Fingerabdrücken an.[294]

Des Weiteren hat sich der EGMR in einigen Fällen mit der Frage befasst, ob Informationen zwingend privater Natur sein müssen, um vom Datenschutz unter Art. 8 EMRK umfasst zu sein. Die benannte Definition der Datenschutzkonvention gibt keine Einschränkung vor, vielmehr können danach jegliche („*any*") Informationen „personenbezogene Daten" sein. Der EGMR hat in seiner frühen Rechtsprechung jedoch vorausgesetzt, dass ein Bezug zum Privatleben bestehen muss.[295] In seiner folgenden Judikatur hat der Gerichthof dieses Kriterium jedoch weit ausgelegt. Im Fall *Uzun v. Germany* haben Ermittlungsbehörden einen GPS-Empfänger an ein Fahrzeug angebracht und die Bewegungen des Beschwerdeführers über einen Zeitraum von drei Monaten gespeichert. Dabei stellt der Gerichtshof fest, dass solch eine GPS-Überwachung im Vergleich zu anderen Überwachungsmethoden zwar keine Informationen über Anschauungen und Gefühle preisgeben. Die Informationen – nämlich die Bewegungen auf den Straßen – sind als solche nicht privat, sondern öffentlich. Allerdings haben die Ermittlungsbehörden die Bewegungen des Beschwerdeführers im öffentlichen Bereich systematisch erfasst, ein entsprechendes Bewegungsprofil erstellt und diese Daten für die Ermittlungen – etwa durch Sichern von Beweismitteln in den aufgesuchten Orten – verwertet. Der Gerichtshof hat hier nicht auf den Inhalt der Informationen abgestellt, sondern vielmehr auf Grundlage der systematischen Erfassung und Verwertung der Daten einen Bezug zum Privatleben und einen Eingriff in Art. 8 angenommen.[296] Zum gleichen Ergebnis kommt der EGMR in Fällen von Videoaufnahmen durch offene Überwachungskameras in öffentlichen Räumen wie Straßen oder Polizeiwachen, wenn die

[292] Ebd., Rn. 72. Im Fall *S. and Marper v. The United Kingdom* wurden die Zellproben, die DNA-Profile sowie die Fingerabdrücke der tatverdächtigen Beschwerdeführer gespeichert. Nach dem Freispruch wurden diese Daten nicht vernichtet, trotz des entsprechenden Ersuchens der Beschwerdeführer.

[293] Ebd., Rn. 71.

[294] Ebd., Rn. 84. Zum Ansatz des EGMR, auf den objektiven Informationsgehalt von Daten abzustellen, siehe *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 63 ff.

[295] EGMR, *Leander v. Sweden*, Rs. 9248/81, 26. März 1987, Series A116, Rn. 48; *Siemen,* Datenschutz als europäisches Grundrecht, S. 88 f.

[296] EGMR, *Uzun v Germany*, Rs. 35623/05, 2. September 2010, Rn. 49–53.

Aufzeichnungen etwa für Videoidentifizierungsverfahren systematisch zusammengestellt[297] sowie zu diesem Zweck sogar an Medien zur Veröffentlichung weitergegeben werden.[298] Im Moment der Aufzeichnung geben die Betroffenen bewusst Informationen in öffentlichen Räumen preis. Allerdings stellt der Gerichtshof auch in diesen Fällen nicht auf den Inhalt der Informationen zum Zeitpunkt der Erfassung ab, sondern stützt sein Ergebnis auf den Prozess der systematischen Erhebung und Verarbeitung der Daten.

Das Vorliegen personenbezogener Daten und die Eröffnung des Schutzbereiches von Art. 8 EMRK hat der EGMR auch für Fälle der dauerhaften Archivierung von öffentlichen Informationen in behördlichen Registern – wie etwa Polizei- und Sicherheitsregistern – angenommen.[299] In diesem Zusammenhang führt der Gerichthof das Argument an, dass Daten durch systematische Speicherung jederzeit abrufbar sind. Damit können solche archivierten Daten auch zu einem Zeitpunkt in der Zukunft abgerufen werden, wenn das entsprechende Geschehnis – wie etwa eine Verurteilung – schon lange in Vergessenheit geraten ist. [300]

Hinsichtlich der Frage, ob Informationen einen Bezug zum Privatleben haben und als „personenbezogene Daten" qualifiziert werden können, stellt der EGMR auch regelmäßig darauf ab, ob eine Person nicht mehr darauf vertraute oder nicht mehr darauf vertrauen durfte, sich in einem rein privaten Bereich zu bewegen („*reasonable expectation of privacy*").[301]

So hat der Gerichtshof im Fall *Perry v. The United Kingdom*, in dem Polizeibeamte gezielte Aufnahmen einer Überwachungskamera zur einer Videomontage zusammengestellt und an Dritte zum Zwecke der Identifikation des Beschwerdeführers als Täter vorgeführt haben, in folgender Weise argumentiert:

> „Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video

[297] EGMR, *Perry v. The United Kingdom*, Rs. 63737/00, 17. Juli 2003, Rep. 2003-IX.

[298] EGMR, *Peck v. The United Kingdom*, Rs. 44647/98, 28. January 2003, Rep. 2003-I. Vgl. auch EGMR *P.G. and J.H. v. The United Kingdom*, Rs. 44787/98, 25. September 2001, Rep. 2001-IX, Rn. 57.

[299] So wurde im Fall *Amann v. Switzerland* [GC], Rs. 27798/95, 16. Februar 2000, Rep. 2000-II eine Karteikarte im Sicherheitsregister des schweizerischen Geheimdienstes mit den persönlichen Daten des Beschwerdeführers angelegt. Im Fall *Rotaru v. Romania* [GC], Rs. 28341/95, 4. Mai 2000, Rep. 2000-V wurden unrichtige Informationen aus weit zurück liegender Vergangenheit über vermeintliche politische Aktivitäten des Beschwerdeführers vom rumänischen Geheimdienst weiterhin verwahrt: „Public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past." Siehe außerdem EGMR, *Segerstedt-Wiberg and Others v. Sweden*, Rs. 62332/00, 6. Juni 2006, Rep. 2006-VII, Rn. 72.

[300] Vgl. EGMR *M.M. v. The United Kingdom*, Rs. 24029/07, 13. November 2012, Rn. 188.

[301] EGMR, *Peev v. Bulgaria*, Rs. 64209/01, 26. Juli 2007, Rn. 38 f; *Perry v. The United Kingdom*, Rs. 63737/00, 17. Juli 2003, Rep. 2003-IX, Rn. 37. *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 77; *Siemen,* Datenschutz als europäisches Grundrecht, S. 126 f.

> identification procedure and, potentially, as evidence prejudicial to his defence at trial. This ploy adopted by the police went beyond the normal or expected use of this type of camera, as indeed is demonstrated by the fact that the police were required to obtain permission and an engineer had to adjust the camera. The permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant."[302]

Aus der Argumentation des Gerichtshofs wird deutlich, dass die Erwartungshaltung des Betroffenen in solchen Fällen ein entscheidendes Kriterium sein kann. Informationen über öffentliche Verhaltensweisen können dem Schutz des Privatlebens nach Art. 8 EMRK unterliegen, wenn die anschließende Verarbeitung dieser Daten die Schwelle dessen, was der Betroffene im Moment der Informationspreisgabe erwarten konnte, überschreiten.

bb. Datenschutzrechtliche Grundprinzipien in Art. 8 EMRK

Der EGMR verweist in seiner einschlägigen Judikatur auch auf die in der Europäischen Datenschutzkonvention verankerten Grundsätze des Datenschutzes und inkorporiert diese somit in den Schutzumfang des Art. 8 EMRK.[303]

In der Entscheidung *S. and Marper v. The United Kingdom* stellt der Gerichtshof fest, dass das nationale Recht einen angemessenen Schutz von personenbezogenen Daten im Sinne der Garantien gem. Art. 8 EMRK vorsehen muss.[304] Das innerstaatliche Recht müsse sicherstellen, dass nur solche personenbezogenen Daten gespeichert werden, die für die Erreichung des angestrebten Zwecks der Datenspeicherung erforderlich sind. Außerdem dürften die Daten nur so lange gespeichert werden, bis der Zweck erreicht ist. Zudem müsse das Recht effektiven Schutz vor Missbrauch und unbefugten Zugriffen garantieren.[305] Der EGMR hat in seiner Spruchpraxis ferner die besondere Schutzbedürftigkeit sensibler Daten, wie etwa DNA- oder Gesundheitsdaten, betont.[306] Unter direktem Verweis auf Art. 5–7 der Europäischen Datenschutzkonvention benennt der Gerichtshof damit die Prinzipien der Rechtmäßigkeit, Zweckbestimmung, Datensparsamkeit, Datensicherheit sowie den besonderen Schutz sensibler Daten.[307]

---

[302] EGMR, *Perry v. The United Kingdom*, Rs. 63737/00, 17. Juli 2003, Rep. 2003-IX, Rn. 41. Vgl. auch EGMR, *Peck v. The United Kingdom*, Rs. 44647/98, 28. January 2003, Rep. 2003-I, Rn. 62; EGMR, *Von Hannover v. Germany*, Rs. 59320/00, 24. Juni 2004, Rep. 2004-VI, Rn. 51.

[303] Vgl. etwa EGMR *M.M. v. The United Kingdom*, Rs. 24029/07, 13. November 2012, Rn. 196.

[304] EGMR, *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 103.

[305] Ebd.

[306] Ebd.; EGMR, *Z. v. Finland*, Rs. 22009/93, 25. Februar 1997, Rep. 1997-I, Rn. 96; *P. and S. v. Poland*, Rs. 57375/08, 30. Oktober 2012, Rn. 128; *I. v. Finland*, Rs. 20511/03, 17. Juli 2008, Rn. 38.

[307] EGMR, *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 103.

III. Zwischenergebnis

Der Schutz der Privatsphäre ist mithin sowohl im IPbpR als auch in der EMRK menschenrechtlich kodifiziert. In Art. 17 IPbpR und Art. 8 EMRK werden die Korrespondenz, die Familie und die Wohnung als Ausprägungen der Privatsphäre ausdrücklich genannt. Der Schutz der Ehre und des guten Rufes wird zudem nur in Art. 17 IPbpR namentlich aufgezählt. Außerdem enthalten beide Artikel einen offenen Auffangtatbestand zum Schutz weiterer Aspekte der Privatsphäre. Der MRA und der EGMR legen die „Korrespondenz“ dynamisch aus und fassen auch moderne Telekommunikationsmittel darunter. Zudem leiten sie den Schutz der personenbezogenen Daten aus „*privacy*“ in Art. 17 IPbpR und aus „*private life*“ in Art. 8 EMRK ab. Im Vergleich zeigt sich jedoch, dass die Spruchpraxis des EGMR zur Auslegung von Art. 8 EMRK und speziell zum Schutz der Korrespondenz und der personenbezogenen Daten deutlich umfassender ist. Insbesondere hinsichtlich der Auslegung des Begriffs „personenbezogen“ hat der Straßburger Gerichthof eine sehr ausführliche Judikatur. Der MRA hat sich mit diesem Thema bislang kaum befasst.

B. Die Vereinbarkeit geheimdienstlicher Telekommunikationsüberwachung mit dem Menschenrecht auf Privatsphäre

Nachfolgend wird zunächst untersucht, inwieweit geheimdienstliche Maßnahmen zur Telekommunikationsüberwachung in die Rechte zum Schutz der Vertraulichkeit der Korrespondenz und der personenbezogenen Daten aus den Art. 17 IPbpR und Art. 8 EMRK eingreifen. Dabei wird auch der Frage nachgegangen, ob auch Gesetze, die solche Überwachungsmaßnahmen regulieren, selbst – ohne konkrete Umsetzung – einen Eingriff in den Schutz der Privatsphäre darstellen können. Anschließend wird die zentrale Frage nach der Vereinbarkeit geheimdienstlicher Telekommunikationsüberwachung mit dem Menschenrecht auf Privatsphäre beleuchtet. Dazu werden die Schrankenregelungen in Art. 17 IPbpR und Art. 8 EMRK vorgestellt. Die einzelnen Voraussetzungen der Schrankenregelungen werden für den konkreten Fall der geheimdienstlichen Telekommunikationsspionage unter Berücksichtigung der sich hieraus ergebenden Besonderheiten dargelegt. Hierfür wird die einschlägige Spruchpraxis des EGMR und des UN-Menschenrechtsausschuss analysiert.

I. Eingriff in den Schutz der Korrespondenz und der personenbezogenen Daten gem. Art. 17 IPbpR und Art. 8 EMRK

Geheimdienstliche Maßnahmen zur Telekommunikationsüberwachung berühren die vertrauliche Übertragung von persönlichen Nachrichten und betreffen damit die von Art. 17 IPbpR und Art. 8 EMRK geschützte Integrität der Korrespondenz. Dabei werden die in Form von Datenpaketen übermittelten Korrespondenzdaten durch die Überwachungsakte erfasst, sodass zugleich der Schutz der personenbezogenen Daten betroffen ist. Denn sowohl die Inhaltsdaten als auch die Metadaten der Korrespondenzen sind in der Regel personenbezogene Daten, wenn die an der Korrespondenz beteiligten Individuen bestimmbar sind. Metadaten sind in der Regel mit der IP-Adresse des Nutzers verbunden, sodass eine Identifizierung der Individuen durchaus möglich ist.[308] Somit ist im Fall der Telekommunikationsüberwachung der Schutzbereich aus Art. 17 IPbpR sowie Art. 8 EMRK hinsichtlich beider Ausprägungen eröffnet. Dies entspricht auch der Sichtweise des EGMR und des Menschenrechtsausschusses.

Der EGMR stellt in seiner Rechtsprechung regelmäßig fest, dass sowohl die Korrespondenz als auch das Privatleben der Individuen betroffen ist:

> „Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a ‚law' that is particularly precise."[309]

Der Menschenrechtsausschuss bezieht in der Entscheidung *Van Hulst v. The Netherlands* seine Argumentation einerseits auf das Schutzgut „*privacy*" gemäß Art. 17 IPbpR.[310] Ohne namentlich den Begriff „*correspondence*" zu verwenden, stützt der Ausschuss seine Rechtsprüfung aber unmissverständlich auch auf den Schutz der Korrespondenz. So spricht der Ausschuss vom „*right to communicate*" des Beschwerdeführers[311] und bestätigt etwa die hohe Bedeutung der „*confidentiality of communiacation*"[312]. Schließlich stellt der Ausschuss in diesem Fall, der die Überwachung der

[308] *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 70 f.

[309] EGMR, *Kopp v. Switzerland*, Rs. 23224/94, 25. März 1998, Rep. 1998-II, Rn. 72. Siehe außerdem EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 41; *Copland v. The United Kingdom*, Rs. 62617/00, 03. April 2007, Rep. 2007-I, Rn. 44; *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008*,* Rn. § 56; *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 118; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 173.

[310] UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.2: „The issue before the Committee is whether the interception and recording of the author's telephone calls with Mr. A.T.M.M. constituted an unlawful or arbitrary interference with his privacy, in violation of article 17 of the Covenant."

[311] Ebd., Rn. 7.8.

[312] Ebd., Rn. 7.6.

Telefonkorrespondenz des Beschwerdeführers und seinem Anwalt zum Gegenstand hatte, folgendes Ergebnis fest:

> „In the light of the foregoing, the Committee concludes that the interference with the author's privacy in regard to his telephone conversations with A.T.M.M. was proportionate and necessary to achieve the legitimate purpose of combating crime".[313]

Im nachfolgenden Unterabschnitt wird in diesem Sinne untersucht, inwieweit die geheimdienstliche Informationsgewinnung in Form der Telekommunikationsausspähung einen Eingriff in den Schutz der Korrespondenz und der personenbezogenen Daten gem. Art. 17 IPbpR und Art. 8 EMRK darstellt.[314]

1. Eingriffe durch geheimdienstliche Überwachungsmaßnahmen

Der direkte Zugriff auf das Telekommunikationsnetzwerk während der Datenübertragung, die Beschaffung von Telekommunikationsdaten aus den Servern von *Service Providern* sowie der Zugriff auf privatgenutzte Telekommunikationsgeräte sind die geheimdienstlichen Überwachungsmaßnahmen, die Gegenstand der vorliegenden Arbeit sind.[315] Im Folgenden wird untersucht, ob und inwieweit diese Überwachungsmaßnahmen in den Schutzbereich der Korrespondenz sowie der personenbezogenen Daten gemäß Art. 17 IPbpR und Art. 8 EMRK eingreifen.

a. Zugriff auf das Telekommunikationsnetzwerk während der Datenübertragung

Art. 17 IPbpR sowie Art. 8 EMRK schützen die Integrität und Vertraulichkeit der Korrespondenz – die Korrespondenz ist mithin vor der Kenntnisnahme durch unbefugte Dritte menschenrechtlich geschützt. Als Abwehrrechte verpflichten sie den Staat, Eingriffe in die Vertraulichkeit der Korrespondenz zu unterlassen. Der Schutz der Vertraulichkeit erstreckt sich dabei insbesondere auf den Prozess der Übertragung vom Absender zum Empfänger. Denn während der Übertragung hat der Absender die Mitteilung bereits aus der Hand gegeben, ohne dass der Adressat diese entgegengenommen hat. Somit befindet sich die Nachricht gerade in diesem Stadium außerhalb des Machtbereiches der Personen und ist damit besonders gefährdet, von Unbefugten abgefangen, eingesehen oder manipuliert zu werden.

Beim geheimdienstlichen Zugriff auf das Telekommunikationsnetzwerk werden mithilfe technischer Vorrichtungen jegliche Daten, die global durch das Glas-

---

[313] Ebd., Rn. 7.10.

[314] Für die menschenrechtliche Untersuchung des Eingriffs und der Rechtfertigung desselben wird allein auf den Akt der Informationsgewinnung abgestellt. Darüber hinausgehende Verarbeitungen der Daten im weiteren Prozess der geheimdienstlichen Arbeitsabläufe, die indes auch eigenständige Eingriffe in das Recht auf Privatsphäre darstellen können, sind nicht Gegenstand dieser Arbeit.

[315] Siehe oben 1. Abschnitt, Unterabschnitt B. III. 2. a.–c.

fasernetz fließen, direkt während der Übertragung abgefangen.[316] Dabei können auch Daten erfasst werden, die keinen Telekommunikationsbezug haben. Denn alle Handlungen im Internet, wie etwa Anfragen in Suchmaschinen oder Online-Käufe, gelangen als Datenpakete in das globale Glasfasernetz. Erst durch gezielte Selektionsmaßnahmen werden die Korrespondenzdaten von anderen Daten herausgefiltert. Letztlich fallen somit Telefonverbindungen, Emailverkehr und andere Formen der modernen elektronischen Telekommunikation ins Netz der Geheimdienste. Die Geheimdienste gewinnen mithin uneingeschränkten Zugriff zu den Daten. Sie können die Telekommunikationsdaten dann beispielsweise entweder sofort – nahezu in Echtzeit – auslesen oder für spätere Analysen zwischenspeichern. Die Vertraulichkeit der abgesendeten Korrespondenzen wird somit durch den geheimdienstlichen Zugriff auf die Telekommunikationsinfrastruktur während des Transfers gestört. Die Geheimdienste erlangen – ohne Einverständnis der Absender und Adressaten – Kenntnis über den Inhalt und die Metadaten der abgefangenen Korrespondenzen. Demnach greift diese Form der Datenerhebung als geheimdienstliche Maßnahme zur Informationsgewinnung in den Schutz der Vertraulichkeit der Korrespondenz gemäß Art. 17 IPbpR und Art. 8 EMRK ein.

Zudem sind diese privaten Kommunikationsinformationen nicht-öffentliche, personenbezogene Daten, die ohne Kenntnis und Einverständnis des Datensubjekts gewonnen und gespeichert werden. Die Identität der korrespondierenden Individuen lässt sich insbesondere aufgrund der IP-Adressen ermitteln. Selbst wenn die Korrespondenz verschlüsselt übertragen wird und der Geheimdienst nicht ohne weiteres auf den Inhalt der Korrespondenz zugreifen kann, wäre ein Eingriff gegeben. Der objektivierte Ansatz des EGMR, den er für den Informationsgehalt von Zellproben und Fingerabdrücken angelegt hat,[317] muss sinngemäß auch für den Bereich verschlüsselter Daten gelten. So kommt es für die Beurteilung der datenschutzrechtlichen Legitimität der Abfangung und Speicherung von Korrespondenzdaten nicht darauf an, inwieweit der Geheimdienst zum Zeitpunkt der Speicherung die Möglichkeit hat, auf alle inkludierten Informationen zuzugreifen. Vielmehr ist auf den objektiven Informationsgehalt der Daten abzustellen, auch wenn diese erst durch aufwendige Dekodierungen für die Geheimdienste nachvollziehbar gemacht werden können. Damit greifen die staatlichen Geheimdienste durch den Zugriff auf das Telekommunikationsnetzwerk auch in das Recht auf Datenschutz gemäß Art. 17 IPbpR und Art. 8 EMRK ein.[318]

Im *General Comment* 16 benennt der Menschenrechtsausschuss das Abfangen der privaten Korrespondenz ausdrücklich als Eingriff in den Schutz der Privatsphäre nach Art. 17 IPbpR:

---

[316] Siehe dazu 1. Abschnitt, Unterabschnitt B. III. 2. a.

[317] Siehe dazu 2. Abschnitt, Unterabschnitt A. II. 2. c. aa.

[318] Vgl. auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 20.

> „Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[319]

Im einschlägigen Fall *Van Hulst v. The Netherlands* hat der Ausschuss festgestellt, dass die Ausspähung und Aufzeichnung der Telefongespräche zwischen dem Beschwerdeführer und seinem Anwalt Eingriffe in Art. 17 IPbpR darstellen.[320] Zudem sind die Fälle der Korrespondenzkontrolle von Strafgefangenen mit der elektronischen Telekommunikationsüberwachung vergleichbar.[321] Denn in beiden Fallkonstellationen findet der staatliche Eingriff auf dem Übertragungsweg der Korrespondenz statt. Der Menschenrechtsausschuss hat in diesen Fällen das Vorliegen eines Eingriffs in Art. 17 IPbpR bejaht.[322] Auch in dem OHCHR-Bericht zum Schutz der Privatsphäre im digitalen Zeitalter wird das Abfangen von elektronischer Telekommunikation als Eingriff in Art. 17 IPbpR qualifiziert.[323]

Der EGMR hat in seiner Jurisprudenz ebenso den Zugriff auf das elektronische Telekommunikationsnetz als einen Eingriff in Art. 8 EMRK bewertet. In einer Reihe von Fällen hat der Gerichtshof festgestellt, dass die Abhörung von Telefongesprächen Eingriffe in den Schutz der Korrespondenz und der personenbezogenen Daten darstellen.[324] Dabei kommt es dem EGMR zufolge auch nicht darauf an, ob die aufgezeichneten Telefonate im Nachhinein auch tatsächlich von den Justizbehörden verwendet werden.[325]

Nach den *Snowden*-Enthüllungen wurden zudem Beschwerden beim EGMR eingereicht, die die weitreichenden Überwachungsform von „*TEMPORA*" thematisieren.[326] Im Fall *Big Brother Watch and Others v. The United Kingdom* rügten die Kläger unter anderem, dass das Abfangen von Telekommunikationsdaten durch den

---

[319] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 8.

[320] UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.4.

[321] Siehe vorangegangenen Unterabschnitt A. I. 2. c.

[322] UN Human Rights Committee, *Boodoo v. Trinidad and Tobago*, No. 721/1996, CCPR/C/74/D/721/1996, 02. April 2002; UN Human Rights Committee, *Miguel Angel Estrella v. Uruguay*, No. 74/1980, U.N. Doc. Supp. No. 40 (A/38/40), 29. März 1983.

[323] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 20.

[324] Vgl. etwa EGMR, *Kruslin v. France*, Rs. 11801/85, 24. April 1990, Serie A 176-A; *Valenzuela Contreras v. Spain*, Rs. 27671/95, 30. Juli 1998, Rep. 1998-V, Rn 46; *Dragojević v. Croatia*, Rs. 68955/11, 15. Januar 2015, Rn. 85.

[325] EGMR, *Kopp v. Switzerland*, Rs. 23224/94, 25. März 1998, Rep. 1998-II, Rn. 53.

[326] Über diese Beschwerden hat die Große Kammer ein gemeinsames Urteil gefällt in der Entscheidung *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021.

britischen Geheimdienst GCHQ unter dem Programm „*TEMPORA*" einen rechtswidrigen Eingriff in ihre Rechte aus Art. 8 EMRK darstellen.[327] Auf Grundlage des *Regulation of Investigatory Powers Act 2000* („RIPA") hat der GCHQ den Datenverkehr an bestimmten Knotenpunkten des transatlantischen Glasfaserkabelnetzes angezapft.[328] Die gewonnenen Daten wurden sodann mithilfe von Selektoren gefiltert. Zur Feststellung eines menschenrechtlichen Eingriffs untergliedert die Große Kammer des EGMR im Urteil zunächst die einzelnen geheimdienstlichen Arbeitsschritte dieser Art der massenhaften Datengewinnung. So werden zunächst jegliche Telekommunikationsdaten abgefangen und zwischengespeichert, aus denen anschließend relevante Informationen gefiltert, analysiert und schließlich für weitere Zwecke gespeichert und weiterverarbeitet werden.[329] Dabei stellt der Gerichtshof hier fest, dass bereits der erste Schritt einen Eingriff in Art 8 EMRK darstelle, auch wenn viele der gewonnenen Daten im nächsten Filterungsprozess aussortiert werden. Dabei sei zwar die Eingriffsintensität im ersten Schritt noch gering, allerdings nehme die Intensität mit jedem Schritt im Verlauf des gesamten geheimdienstlichen Verarbeitungsprozess zu.[330] Damit bestätigte der Gerichtshof seine bisherige Spruchpraxis, dass für das Vorliegen eines Eingriffes die tatsächliche Verwendung der gewonnenen Informationen nicht entscheidend ist.[331]

b. Beschaffung von Telekommunikationsdaten aus Servern von *Service Providern*

Eine weitere geheimdienstliche Maßnahme der Telekommunikationsüberwachung ist die Beschaffung von Telekommunikationsdaten mithilfe von *Service Providern*. Dazu können Internet- und Telekommunikationsdienstleister etwa aufgrund von Gesetzen zur Herausgabe der Daten auf ihren Servern oder zur Ermöglichung des geheimdienstlichen Zugriffs verpflichtet werden.[332] Auch ist eine freiwillige Kooperation der Dienstleister mit den Geheimdiensten denkbar. Zudem können die staatlichen Gesetze eine Vorratsdatenspeicherung durch die *Service Provider* vorschreiben,

---

[327] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 13, 277 ff.. Zum Überwachungsprogramm „*TEMPORA*" siehe oben 1. Abschnitt, Unterabschnitt B. III. 2. a.

[328] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 19.

[329] Ebd., Rn. 325.

[330] Ebd., Rn. 330. Dies geht ebenso aus der Entscheidung EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 244 hervor: „The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses".

[331] Dazu bereits oben der Verweis auf EGMR, *Kopp v. Switzerland*, Rs. 23224/94, 25. März 1998, Rep. 1998-II, Rn. 53.

[332] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 18.

um im Bedarfsfall – etwa zu Ermittlungszwecken – einen Zugriff auf die gespeicherten Daten durch staatliche Behörden zu ermöglichen.[333]

Bei dieser Form der geheimdienstlichen Datenbeschaffung findet die staatliche Maßnahme jeweils zu einem Zeitpunkt statt, bei dem die Übertragung bereits beendet ist. Von der Absendung bis zum Empfang der Nachricht – während des gesamten Übertragungsprozesses – greift der Staat nicht in die Vertraulichkeit der Korrespondenz ein. Erst nachdem die Geheimdienste Zugang zu den Servern der Dienstleister haben oder die Verbindungsdaten von den *Service Providern* erhalten, erlangen sie Kenntnis über die Korrespondenzen der Benutzer. Der Schutz der Vertraulichkeit der Korrespondenz endet jedoch nicht mit dem Abschluss der Übertragung. Vielmehr erstreckt sich der Schutz gemäß Art. 17 IPbpR sowie Art. 8 EMRK auch auf bereits empfangene Nachrichten sowie die entsprechenden Verkehrsdaten.[334] So hat der EGMR etwa im Fall *Malone v. The United Kingdom* befunden, dass die Herausgabe der von den Anbietern registrierten Telefon-Verbindungsdaten an die Polizei einen Eingriff in Art. 8 EMRK darstellt.[335]

Neben einem Eingriff in den Schutz der Vertraulichkeit der Korrespondenz, greift auch diese Form der Überwachung zudem in den Schutz personenbezogener Daten gemäß Art. 17 IPbpR und Art. 8 EMRK ein. Die Benutzer von Telekommunikationsdienstleistungen willigen regelmäßig darin ein, dass die *Service Provider* die Verbindungsdaten im Zuge der Bereitstellung ihrer Kommunikationsdienste kurzzeitig speichern.[336] Dieses Verfahren unterliegt konkreten Regulierungen über Speicherungsfristen und der Löschung der Daten nach Abwicklung der Dienste. Insofern erfolgt – innerhalb des Rahmens der konkreten Vereinbarungen und Regulierungen – die Preisgabe von Kommunikationsdaten durch die Individuen an die Anbieter auf freiwilliger Basis. Allerdings erstreckt sich dieses Einverständnis in der Regel nicht auf eine Weitergabe an einen staatlichen Geheimdienst. Werden die *Service Provider* indes verpflichtet, die Kommunikationsdaten ihrer Benutzer für den Geheimdienst offen zu legen, so ist diese Kenntnisnahme durch den Geheimdienst eben nicht mehr vom Einverständnis des Individuums gedeckt. Selbst wenn es sich um öffentliche Korrespondenzen – etwa auf *Facebook* – handelt, wäre der Schutz der personenbezogenen Daten tangiert. Denn hier ist die Argumentation des EGMR im Fall *Perry v. The United Kingdom* sinngemäß anzuwenden.[337] Die Nutzer

[333] Siehe 1. Abschnitt, Unterabschnitt B. III. 2. b.
[334] Siehe dazu bereits oben 2. Abschnitt, Unterabschnitt B. I. 1. b.
[335] EGMR, *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 84.
[336] Möchte ein Internetnutzer beispielsweise eine Emailadresse einrichten, muss er in die Datenschutzerklärung des jeweiligen Anbieters durch Anklicken des entsprechenden Feldes einwilligen. Anderenfalls kann er diesen Dienst nicht nutzen. In dieser Erklärung wird der Umgang mit den Daten des Nutzers erläutert, etwa die Speicherung, Löschung und Weitergabe der personenbezogenen Daten. So willigen Googlemail-Nutzer etwa in die Verarbeitung ihrer Daten entsprechend der Datenschutzerklärung von Google (abrufbar unter https://policies.google.com/privacy?hl=de&gl=DE [zuletzt abgerufen am 02.12.2021]) ein.
[337] EGMR, *Perry v. The United Kingdom*, Rs. 63737/00, 17. Juli 2003, Rep. 2003-IX, Rn. 41. Siehe zur Argumentation des EGMR oben 2. Abschnitt, Unterabschnitt A. II. 2. c. aa.

dieser *Social Media* gehen bei der Erstellung dieser öffentlichen Korrespondenzen nicht davon aus, dass diese in systematischer Weise an Geheimdienste weitergegeben werden. Die Weitergabe dieser öffentlichen Daten an die Geheimdienste und die anschließende geheimdienstliche Verarbeitung dieser Daten überschreitet die Schwelle dessen, was der Betroffene im Moment der Informationspreisgabe erwarten konnte.

Die Inanspruchnahme von *Service Providern* zur Gewinnung von Telekommunikationsdaten war auch Gegenstand des EGMR-Falles *Roman Zakharov v. Russia.*[338] In diesem Fall verpflichteten nationale Vorschriften die Mobilfunknetzbetreiber u.a. zur Installation von Geräten, die eine Durchführung von Suchaktivitäten in den Mobilfunkverbindungen durch Sicherheitsdienste ermöglichten.[339] Die zentrale Frage dieser Entscheidung war, ob allein nationale Vorschriften über solche Überwachungsmaßnahmen für eine Verletzung der Rechte des Beschwerdeführers aus Art. 8 EMRK genügten. Dies hat der EGMR ausführlich geprüft, letztlich bejaht und schließlich unter Würdigung aller Umstände des Falles eine Verletzung von Art. 8 EMRK festgestellt.[340] Aus dieser Entscheidung geht letztlich hervor, dass die Informationsgewinnung im Wege der Verpflichtung von Service Providern zur Erlangung von Telekommunikationsdaten grundsätzlich einen Eingriff in Art. 8 EMRK darstellen kann. Zwar geht es an dieser Stelle nicht um die Frage des Eingriffs aufgrund von Gesetzen. Dies wird an späterer Stelle beleuchtet.[341] Wenn allerdings bereits ein Gesetz mit solch einer Verpflichtungsregelung einen Eingriff darstellen kann, wie vom EGMR in diesem Urteil festgestellt, dann gilt dies erst recht für den Fall der tatsächlichen Durchführung dieser Art der Erlangung von Telekommunikationsdaten. Dies wird durch die Entscheidung *Big Brother Watch and Others v. The United Kingdom* bestätigt, da hier der EGMR hinsichtlich der geheimdienstlichen Informationsgewinnung durch *Service Provider* vom Vorliegen eines Eingriffs unproblematisch ausgeht.[342]

c. Zugriff auf private Telekommunikationsgeräte

Eine weitere Form des Eingriffs in den Schutz der Korrespondenz und der personenbezogenen Daten liegt schließlich hinsichtlich der dritten Fallgruppe der Telekommunikationsausspähung – das Hacken von privaten Telekommunikationsgeräten – vor.[343] Hierbei verschaffen sich die Geheimdienste durch spezielle Spionagesoftware oder eingebauten Sendern zur heimlichen Datenübertragung direkten Zugang zu privatgenutzten Telekommunikationsgeräten. Mithilfe dieser Spionage-

[338] EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015.
[339] Ebd., Rn. 109 ff.
[340] Ebd., Rn. 302 ff.
[341] Siehe dazu 2. Abschnitt, Unterabschnitt B. I. 2.
[342] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 518 f., 522.
[343] Siehe UN Human Rights Committee, Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37.

systeme sind sie in der Lage, in den unterschiedlichen Stadien der Korrespondenzübermittlung einzugreifen und die Korrespondenzen umfassend auszuspähen. Das zeitgleiche Mitverfolgen von Telefongesprächen oder Chats ist genauso möglich, wie der Zugriff auf gespeicherte Nachrichten.[344] Bei dieser Form der Überwachung gewinnt der Geheimdienst die Informationen direkt beim Spionage-Objekt (Individuum), ohne auf das allgemeine Telekommunikationsnetzwerk oder den Datenpool von *Service Providern* zurückgreifen zu müssen.

Diese Fallgruppe ist vergleichbar mit Fällen der Beschlagnahme von privaten Computern. Der Unterschied besteht indes darin, dass der Geheimdienst keine physische Kontrolle über das Gerät ausübt, sondern vielmehr über einen virtuellen Fernzugang verfügt. Diese Art der Überwachung erreicht zwar nicht die enorme Breitenwirkung, die insbesondere beim geheimdienstlichen Zugriff auf das globale Telekommunikationsnetzwerk erzielt wird. So geraten im letzteren Fall in kürzester Zeit unzählige Individuen in den Wirkungsradius dieses Überwachungssystems. Dahingegen sind aufgrund des relativ hohen Aufwandes eines geheimdienstlichen Direktzugangs auf persönliche Telekommunikationsgeräte im Vergleich weniger Individuen hiervon betroffen. Die Tiefenwirkung – d.h. die Eingriffsintensität – dieser Überwachungsmethode ist jedoch erheblich.[345] Denn der Geheimdienst gewinnt mit dem direkten Zugriff auf persönliche Telekommunikationsgeräte ein umfassendes Profil der betroffenen Personen. Der direkte Zugang zu den Computern oder Mobiltelefonen der Individuen offenbart jegliche Nachrichten, die von dem betroffenen Gerät verschickt, empfangen sowie hierauf gespeichert wurden. Die Geheimdienste erlangen Kenntnis über die Inhalte sowie die Metadaten der Nachrichten. Somit kann kein Zweifel daran bestehen, dass diese Formen der Telekommunikationsüberwachung Eingriffe in den Schutz der Korrespondenz und der personenbezogenen Daten gemäß Art. 17 IPbpR und Art. 8 EMRK darstellen.

2. Eingriff durch nationale Gesetze zur Telekommunikationsüberwachung

Spezifisches Merkmal geheimdienstlicher Telekommunikationsüberwachung ist ihre verdeckte Ausführung. Betroffene Individuen bemerken in aller Regel nicht, dass ihre Telekommunikation von Geheimdiensten überwacht wird. Selbst im Falle des Verdachts einer Überwachung sind Individuen zumeist nicht in der Lage, die Durchführung der geheimen Überwachung nachzuweisen und demzufolge die vermutliche Überwachungspraxis etwa vor Gerichten mit Aussicht auf Erfolg geltend zu machen.[346] Die geheimdienstlichen Maßnahmen zur Telekommunikationsüberwachung basieren allerdings meist auf nationalen Gesetzen, die den Geheimdiensten mehr oder weniger umfassende Überwachungsbefugnisse gewähren. Der

[344] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 38.
[345] Eingehend zur Eingriffsintensität siehe 2. Abschnitt, Unterabschnitt B. II. 4. a.
[346] So argumentiert auch der EGMR in der Entscheidung *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 36.

Anwendungsbereich solcher Gesetze kann einen weiten Kreis von potenziell betroffenen Individuen einschließen. Insofern stellt sich die Frage, inwieweit die potenziell betroffenen Individuen einen Eingriff in den Schutz der Vertraulichkeit ihrer Korrespondenz und in den Schutz der personenbezogenen Daten aufgrund der zugrundeliegenden nationalen Gesetze zur Telekommunikationsüberwachung geltend machen können, ohne sich auf eine tatsächliche Durchführung der Überwachung im Einzelfall berufen zu müssen.

a. Die Spruchpraxis des EGMR

Der EGMR hat sich in den vergangenen 30 Jahren in einigen Fällen mit der Frage beschäftigen müssen, inwieweit im Kontext der geheimdienstlichen Telekommunikationsüberwachung allein Gesetze einen Eingriff in Art. 8 EMRK darstellen können. Die sich damit überschneidende und für die Zulässigkeit der Beschwerde relevante Frage nach der Opfereigenschaft der Beschwerdeführer im Sinne des Art. 34 EMRK prüft der Gerichtshof in diesen Fallkonstellationen indes nicht getrennt, sondern begutachtet dies in Verbindung mit der Eingriffsprüfung im Rahmen der Begründetheit.[347] Der EGMR führt grundsätzlich keine abstrakte Normenkontrolle durch, sondern prüft vielmehr, ob die konkrete Anwendung von Gesetzen im Einzelfall Konventionsrechte verletzen.[348] Jedoch lässt er unter Berücksichtigung der spezifischen Umstände im besonderen Fall der geheimdienstlichen Überwachungsmaßnahmen eine Ausnahme zu. So hat der EGMR im Fall *Klass and Others v. Germany* grundlegend festgestellt, dass hinsichtlich der Praxis geheimer Telekommunikationsüberwachung für die Beurteilung der Opfereigenschaft und eines Eingriffs in Art. 8 EMRK auf die zugrundeliegenden Gesetze abgestellt werden kann:

> „Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to ‚(claim) to be the victim of a violation‘ of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions."[349]

In der Folge hat der EGMR in weiteren Fällen festgestellt, dass die bloße Existenz von Gesetzen, die geheime Überwachungsmaßnahmen zulassen, Eingriffe in die

---

[347] Siehe etwa EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 149 ff.

[348] EGMR, *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], Rs. 47848/08, 17. Juli 2014, Rep. 2014, Rn. 101 m.w.N.

[349] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 38. Siehe außerdem Rn. 41 dieser Entscheidung: „in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menance of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an ‚interference by a public authority'."

Rechte aller in den Anwendungsbereich der Gesetze fallenden Individuen darstellen.[350] In anderen Entscheidungen hat der Gerichtshof hingegen eine restriktivere Argumentation formuliert, wonach der Beschwerdeführer nachweisen müsse, dass mit hinreichender Wahrscheinlichkeit („*reasonable likelihood*") seine Telekommunikation von den geheimdienstlichen Überwachungsmaßnahmen konkret betroffen war.[351] Zudem hat der Gerichtshof im Fall *Kennedy v. The United Kingdom* hinzugefügt, dass die Verfügbarkeit von nationalen Rechtsbehelfen als wichtiges Kriterium in diesen Fällen zu berücksichtigen ist.[352]

Diese unterschiedlichen Argumentationsstränge in seiner Jurisprudenz hat der EGMR im Fall *Roman Zakharov v. Russia* zusammengeführt und harmonisiert sowie letztlich die entscheidenden Kriterien für die Beurteilung eines Eingriffs in entsprechenden Fallkonstellationen hervorgehoben.[353] So sei als erstes Kriterium der personale Geltungsbereich des Gesetzes zur geheimen Telekommunikationsüberwachung heranzuziehen.[354] Dabei ist der Frage nachzugehen, inwieweit der konkrete Beschwerdeführer in den normativen Anwendungsbereich des Gesetzes fällt. Gilt das Gesetz für eine bestimmte Personengruppe, unter die der Beschwerdeführer fällt, oder betrifft es unterschiedslos alle Telekommunikationsnutzer, so spricht dies für eine Annahme eines Eingriffs durch das Gesetz. Darüber hinaus bewertet der EGMR – im Sinne seiner *Kennedy*-Rechtsprechung – als zweites Kriterium die Verfügbarkeit von effektiven Rechtsbehelfen auf nationaler Ebene:

> „As the Court underlined in Kennedy, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified […]."[355]

Der Gerichtshof argumentiert hier folglich mit dem allgemeinen Verdacht der Überwachung, der aufgrund des Mangels individueller Rechtsbehelfe unter der gesamten Bevölkerung entsteht. Wenn demzufolge das nationale Rechtssystem den Individuen, die eine Überwachung ihrer Korrespondenz vermuten, keine Rechtsmittel zur Anfechtung der geheimdienstlichen Maßnahmen gewähren, so stellt die Gefahr einer potenziellen Überwachung als solche einen Eingriff in den Schutz der Privatsphäre nach Art. 8 EMRK dar. Das Individuum müsse in solch einem Fall die

[350] EGMR, *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 64; EGMR, *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008, Rn. 56, 57. Siehe auch EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 168 m.w.N.

[351] EGMR *Halford v. The United Kingdom*, Rs. 20605/92, 25. Juni 1997, Rep. 1997-III, Rn. 55–57; vgl. auch EGMR, *Iliya Stefanov v. Bulgaria*, Rs. 65755/01, 22. Mai 2008, Rn. 49–50.

[352] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 124.

[353] EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn.170 ff.

[354] Ebd., Rn. 171.

[355] Ebd.

konkrete Wahrscheinlichkeit einer Überwachung dem Gerichtshof zufolge nicht mehr nachweisen. Denn in diesen Fällen bestehe ein erhöhter Kontrollbedarf durch den EGMR. Sind in einem Staat hingegen effektive Rechtsmittel verfügbar, so könne sich das Individuum nur dann vor dem EGMR direkt gegen die Gesetze wenden, wenn er mit hinreichender Wahrscheinlichkeit darlege, dass er von Überwachungsmaßnahmen betroffen war.[356]

b. Die Spruchpraxis des MRA

Der UN-Menschenrechtsausschuss hat zwar keine vergleichbar umfangreiche Rechtsprechung zu dieser Fragestellung wie der EGMR. Insbesondere hat der Ausschuss bislang in keiner Individualbeschwerde explizit darüber entscheiden müssen, ob Gesetze zur Telekommunikationsüberwachung Eingriffe in den Schutz der Vertraulichkeit der Korrespondenz darstellen. Allerdings hat der Ausschuss in anderen Fallkonstellationen durchaus für die Feststellung eines Eingriffs in Art. 17 IPbpR auf Gesetze abgestellt.[357] Im Fall *Toonen v. Australia* hat der Menschenrechtsausschuss ein strafrechtliches Verbot einvernehmlicher homosexueller Aktivitäten, das seit Jahren in der Praxis nicht mehr angewendet wurde, als Eingriff in das Privatleben gemäß Art. 17 IPbpR qualifiziert:

> „The Committee considers that sections 122 (a) and (c) and 123 of the Tasmanian Criminal Code ‚interfere' with the author's privacy, even if these provisions have not been enforced for a decade. In this context, it notes that the policy of the Department of Public Prosecutions not to initiate criminal proceedings in respect of private homosexual conduct does not amount to a guarantee that no actions will be brought against homosexuals in the future […]. The continued existence of the challenged provisions therefore continuously and directly ‚interferes' with the author's privacy."[358]

Darüber hinaus hat der Ausschuss im Fall *Aumeeruddy-Cziffra et al v. Mauritius* hinsichtlich der mauritischen Gesetzeslage, die eine unterschiedliche Behandlung von ausländischen Witwen und Witwern mauritischer Ehepartner in Bezug auf das Aufenthaltsrechts vorsah, eine Verletzung von Art. 17 IPbpR festgestellt:

> „In the present cases, not only the future possibility of deportation, but the existing precarious residence situation of foreign husbands in Mauritius represents, in the opinion of the Committee, an interference by the authorities of the State party with the family life of the Mauritian wives and their husbands. The statutes in question have rendered it uncertain for the families

[356] Ebd.

[357] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 3.46 ff.

[358] UN Human Rights Committee, *Toonen v. Australia*, No. 488/1992, CCPR/C/50/D/488/1992, 31. März 1994, Rn. 8.2.

> concerned whether and for how long it will be possible for them to continue their family life by residing together in Mauritius."[359]

Interessanterweise argumentiert der Menschenrechtsausschuss sowohl im Fall *Toonen v. Australia*, als auch im Fall *Aumeeruddy-Cziffra et al v. Mauritius* mit der unsicheren Lage, die für die Betroffenen infolge der bloßen Existenz der Gesetze entstünde. Diese Argumentation des Ausschusses muss konsequenterweise ebenso für Gesetze, die eine geheimdienstliche Telekommunikationsüberwachung legitimieren, gelten. So sind Personen, die potenziell von Überwachungsgesetzen betroffen sind, mit der Unsicherheit konfrontiert, ob die Integrität und Vertraulichkeit ihrer Korrespondenzen gewahrt wird oder aber Gegenstand von Überwachungsmaßnahmen sind. Eben diese Unberechenbarkeit führt zu einer vorsorglichen Selbstzensur und einer gegen sich selbst gerichteten Freiheitsbeschränkung. Somit können nationale Gesetze über die Überwachung der Telekommunikation von Individuen – im Sinne der dargelegten Judikatur des Ausschusses – Eingriffe in den Schutz der Vertraulichkeit der Korrespondenz und in den Schutz der personenbezogenen Daten gemäß Art. 17 IPbpR darstellen.[360] Dies geht auch ausdrücklich aus dem OHCHR-Bericht zum Schutz der Privatsphäre im digitalen Zeitalter hervor, wobei in diesem Zusammenhang das Hochkommissariat auf die EGMR-Entscheidung *Weber and Saravia v. Germany*[361] verweist.[362]

c. Zwischenergebnis und Stellungnahme

Der EGMR hat in seiner Spruchpraxis die Möglichkeit eines Eingriffs durch Telekommunikationsgesetze eindeutig anerkannt und zudem konkrete Kriterien zur Beurteilung des Vorliegens eines Eingriffs im Einzelfall entwickelt. Die einschlägige Spruchpraxis des MRA bezieht sich zwar nicht direkt auf Eingriffe durch Telekommunikationsgesetze. Allerdings befürwortet der Ausschuss generell die Möglichkeit von staatlichen Eingriffen in den Schutzbereich von Menschenrechten aufgrund von Gesetzen. Der Judikatur beider Spruchkörper ist zuzustimmen. Denn Gesetze zur Telekommunikationsüberwachung beeinflussen das Verhalten der potenziell betroffenen Personen. Die Kenntnis über die mögliche Überwachung führt dazu, dass die Individuen ihr Telekommunikationsverhalten regulieren und sich gar selbst zensieren. Um einer Überwachung zu entgehen, vermeiden die Personen etwa bestimmte Gesprächsinhalte, meiden Korrespondenzen zu bestimmten – nach ihrer Einschätzung „verdächtigen" – Personengruppen oder verzichten sogar weitgehend auf die Nutzung der modernen Telekommunikation. Sie beschränken somit

---

[359] UN Human Rights Committee, *Aumeeruddy-Cziffra et al v. Mauritius*, No. 35/1978, CCPR/C/12/D/35/1978, 09. April 1994, Rn. 9.2 (b) 2 (i) 3.

[360] Vgl. auch *Georgieva,* The Right to Privacy under Fire, S. 117.

[361] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI.

[362] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 20.

selbst ihre menschenrechtlichen Freiheiten. Angesichts dessen können im Einzelfall auch Gesetze zur Telekommunikationsüberwachung durchaus Eingriffe in Art. 17 IPbpR und Art. 8 EMRK darstellen, ohne dass es einer konkreten Durchführung von Überwachungsmaßnahmen im Einzelfall bedarf.

II. Voraussetzungen für die Vereinbarkeit der Telekommunikationsüberwachung mit dem Menschenrecht auf Privatsphäre

1. Schrankenregelungen in Art. 17 IPbpR und Art. 8 EMRK

Artikel 17 IPbpR enthält keine ausdrückliche Schrankenregelung.[363] Allerdings kann aus dem Wortlaut der Norm abgeleitet werden, dass unter bestimmten Voraussetzungen Begrenzungen dieses Menschenrechts legitim sind. So verbietet Art. 17 Abs. 1 IPbpR explizit rechtswidrige und willkürliche Eingriffe in den Schutzbereich der Privatsphäre („*arbitrary or unlawful interference*").[364] Im Umkehrschluss sind folglich Beschränkungen mit Art. 17 IPbpR vereinbar, sofern diese nicht „*unlawful*" oder „*arbitrary*" sind. Der Menschenrechtsausschuss hat in seiner Spruchpraxis diese zentralen Begriffe ausgelegt und damit die Schranken des Rechts auf Privatsphäre gemäß Art. 17 IPbpR konkretisiert. So geht aus dem Begriff „*unlawful*" hervor, dass staatliche Eingriffe nur auf Grundlage von Gesetzen erfolgen dürfen, die ihrerseits mit den Bestimmungen und Zielen des Paktes vereinbar sind.[365] Aus dem Begriff „*arbitrary*" leitet der Ausschuss indes ab, dass auch gesetzlich vorgesehene Eingriffe mit den Bestimmungen des Paktes im Einklang stehen und verhältnismäßig sein müssen.[366] Ausgehend von dieser Lesart und der hierauf basierenden Spruchpraxis ist heute unstreitig, dass Eingriffe in Art. 17 IPbpR gerechtfertigt sind, wenn sie auf Grundlage einer gesetzlichen Regelung geschehen, ein mit dem Pakt im Einklang stehendes Ziel verfolgen und schließlich im Einzelfall verhältnismäßig sind.[367]

---

[363] In der Entstehungsphase des IPbpR wurde für den Art. 17 vorgeschlagen, eine ausdrückliche Schrankenregelung hinzuzufügen. Allerdings hat die Mehrheit der Staaten dagegen votiert. Siehe *Bossuyt,* Guide to the „Travaux Préparatoires", S. 381. Vgl. dazu auch *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 76 f.

[364] Der Begriff „*arbitrary*" wird nur im Zusammenhang der Schutzgüter Privatleben, Familie, Wohnung und Korrespondenz genannt. Für die Ehre und den Ruf werden hingegen allein unrechtmäßige Beeinträchtigungen untersagt – der Begriff „*arbitrary*" wird in diesem Zusammenhang nicht erwähnt. Somit ist die Schrankenregelung für Eingriffe in Privatleben, Familie, Wohnung und Korrespondenz strenger als die Regelung für Ehre und Ruf. Siehe dazu auch *Nowak*, CCPR Commentary, Art. 17, S. 381, Rn. 9.

[365] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 3.

[366] Ebd., Rn. 4.

[367] *Nowak*, CCPR Commentary, Art. 17, S. 383, Rn. 12; UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004,

Im Gegensatz zu Art. 17 IPbpR enthält Art. 8 Abs. 2 EMRK eine ausdrückliche Schrankenregelung:

> „There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Danach sind Eingriffe in Art. 8 Abs. 1 EMRK gerechtfertigt, wenn diese gesetzlich vorgesehen sind und eines der in Absatz zwei explizit aufgezählten Ziele verfolgen. Darüber hinaus muss der Eingriff „in einer demokratischen Gesellschaft notwendig", d.h. verhältnismäßig sein.[368]

Auch wenn der Wortlaut der beiden Artikel dies auf den ersten Blick nicht vermuten lässt, so implizieren Art. 17 IPbpR und Art. 8 EMRK jedoch im Wesentlichen gleiche Voraussetzungen für die Rechtfertigung von Eingriffen in den Schutzbereich des Menschenrechts auf Privatsphäre. In diesem Sinne wird im Folgenden für beide Artikel gemeinsam geprüft, inwieweit geheimdienstliche Maßnahmen zur Telekommunikationsüberwachung diesen Voraussetzungen genügen. Dabei wird die Jurisprudenz beider Spruchkörper herangezogen und an entsprechenden Stellen werden paktspezifische Besonderheiten der Art. 17 IPbpR und Art. 8 EMRK hervorgehoben.

2. Gesetzliche Grundlage

Die nationalen Gesetze, die den staatlichen Maßnahmen zur Telekommunikationsüberwachung zugrunde liegen, müssen ihrerseits mit den Bestimmungen des jeweiligen Paktes im Einklang stehen und zudem die qualitativen Anforderungen der allgemeinen Zugänglichkeit und hinreichenden Bestimmtheit nach Art. 17 IPbpR und Art. 8 EMRK erfüllen.

Rn. 7.3; *Leonid Raihman v. Latvia*, No. 1621/2007, CCPR/C/100/D/1621/2007, 30. November 2010, Rn. 8.3. Siehe auch Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Ben Emmerson, A/69/397, 23. September 2014, Rn. 30.

[368] *Grabenwarter,* European Convention on Human Rights, Art. 8, S.204 ff., Rn. 42 ff.

a. *Accessibility*: Die Zugänglichkeit der gesetzlichen Grundlage

Die allgemeine Zugänglichkeit der Rechtsgrundlage für staatliche Eingriffe in das Recht auf Privatsphäre wird von Art. 17 IPbpR vorausgesetzt.[369] Der Menschenrechtsausschuss hat in einigen *Concluding Observations* auf dieses Erfordernis ausdrücklich hingewiesen.[370] In der umfangreichen Rechtsprechung des EGMR wird die allgemeine Zugänglichkeit der gesetzlichen Grundlage („*Accessibility of domestic law*") als eines der allgemeinen Voraussetzungen für die Rechtfertigung von Eingriffen in Art. 8 EMRK regelmäßig benannt.[371]

So sind die Staaten verpflichtet, Gesetze, die Eingriffe in das Menschenrecht auf Privatsphäre regeln, offiziell zu veröffentlichen und damit für die allgemeine Bevölkerung zugänglich zu machen. Die allgemeine Zugänglichkeit von Gesetzen schafft Transparenz.[372] Potenziell betroffene Individuen müssen darüber Kenntnis haben, dass ihre Privatsphäre auf Grundlage eines Gesetzes eingeschränkt werden kann. Wenn die zugrundeliegenden Gesetze geheim sind, wären Individuen ohne Vorwarnung den Eingriffen ausgesetzt.[373] Darüber hinaus wäre in der Folge die Gefahr einer missbräuchlichen Anwendung dieses Gesetzes erhöht. Allerdings spielt gerade im Bereich der geheimdienstlichen Überwachung die Geheimheit der Maßnahmen eine zentrale Rolle und wird von den Staaten als Argument für die Effektivität der Maßnahmen – etwa für Ermittlungszwecke – betont. Vor diesem Hintergrund sind häufig im Bereich geheimdienstlicher Maßnahmen die zugrundeliegenden Gesetze zumindest teilweise nicht öffentlich zugänglich. Letztlich darf im Spannungsfeld zwischen Transparenz staatlichen Handelns und dem Argument der Überwachungseffektivität jedoch nicht das berechtigte Vorhersehbarkeitsinteresse der potenziell betroffenen Individuen gänzlich außer Acht gelassen werden. Der EGMR hat angesichts dessen richtigerweise festgestellt, dass im geheimdienstlichen Bereich die Staaten nicht jegliche Details ihrer Bestimmungen für geheime Überwachungsoperationen veröffentlichen müssten. So sei es im Bereich geheimdienstlicher Überwachung unvermeidbar, dass „*below the waterline*" Regulierungen existierten. Entscheidend sei in diesen Fällen, ob die öffentlich zugänglichen Gesetze in hinreichendem Maße Vorhersehbarkeit schufen, um die Gefahr eines Macht-

[369] Vgl. *Nowak*, CCPR Commentary, Art. 17, S. 382, Rn. 11. Nowak leitet dies aus Art. 17 Abs. 2 IPbpR ab: „Moreover, it follows from Art. 17 (2) that authorization to interfere with privacy must be based on generally accessible provisions *of law* (in the formal sense) proclaimed prior to interference". Vgl. auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 35.

[370] Siehe etwa UN Human Rights Committee, Concluding observations: Hungary, CCPR/C/HUN/CO/6, 9. Mai 2018, Rn. 44; Concluding observations: United States of America, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22; UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24.

[371] Vgl. EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 59 m.w.N.

[372] *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 135.

[373] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 35.

missbrauches zu minimieren.[374] Im Fall *Big Brother Watch and Others v. The United Kingdom* hat der Gerichtshof zudem klargestellt, dass das Prinzip der Zugänglichkeit auch gewahrt sein kann, wenn die Rechtsgrundlagen sehr komplex und auf den ersten Blick unklar sind. In diesem Fall verwies der Gerichtshof auf die begleitenden Anwendungsleitlinien, die als parlamentarisch genehmigtes öffentliches Dokument von der britischen Regierung online und in gedruckter Form veröffentlicht wurden.[375] Hier sind die Einzelheiten über die Funktionsweise des Überwachungssystems in der Praxis beschrieben. Insofern hat auch hier der EGMR das Vorliegen der *Accessibility* bestätigt.[376]

b. *Foreseeability*: Die Bestimmtheit der gesetzlichen Grundlage

Art. 17 IPbpR und Art. 8 EMRK setzen voraus, dass die Gesetzesgrundlage eines Eingriffs hinreichend bestimmt sein muss. Im *General Comment* 16 hat der Menschenrechtsausschuss dazu konkretisierend ausgeführt, dass das einschlägige Gesetz detailliert die genauen Voraussetzungen, unter welchen Eingriffe zulässig sind, nennen müsse.[377] Insbesondere in der Jurisprudenz des EGMR hat sich in diesem Zusammenhang der Begriff „*foreseeability*" etabliert.[378] Die entsprechenden Gesetze müssten demnach soweit bestimmt sein, dass die Individuen die Handlungsbefugnisse des Staates und die Konsequenzen, die sich aus der Anwendung der Gesetze ergeben, vorhersehen können.[379] Im Rahmen von geheimdienstlichen Maßnahmen zur Telekommunikationsüberwachung beruht die einschlägige Jurisprudenz beider Spruchkörper auf der Prämisse, dass im Sinne der Rechtsstaatlichkeit der Schutz vor staatlicher Willkür und vor Machtmissbrauch durch weitgehend konkrete Gesetzesgrundlagen gewährleistet werden muss.[380] Dabei stellt sich jedoch gerade im Kontext geheimdienstlicher Überwachung die Frage, inwieweit das Erfordernis der Vorhersehbarkeit gilt. Denn für eine erfolgsversprechende Ausspähung kommt es aus Staatensicht gerade auf die geheime und vom Individuum unbemerkte

---

[374] Siehe EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 243–244, 247; *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 64; *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 159.

[375] Es handelt sich hiebei um das Interception of Communications Code of Practice, das mit dem Regulation of Investigatory Powers Act 2000 („RIPA") zusammenhängt. Siehe EGMR, Big Brother Watch and Others v. The United Kingdom [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 93 ff., 366.

[376] Ebd., Rn. 366.

[377] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 8.

[378] Vgl. EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 59 m.w.N.

[379] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 151. Siehe auch *Nardell,* Levelling Up: Data Privacy and the ECHR, in Gutwirth/Poullet/De Hert (Hrsg.), Data Protection in a Profiled World, S. 46. Hinsichtlich Art. 17 IPbpR vgl. *Nowak*, CCPR Commentary, Art. 17, S. 383, Rn. 12.

[380] Ebd; *Schabas,* The European Convention on Human Rights, Art. 8, S. 403. Vgl. auch EGMR, *Malone v. The United Kingdom,* Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 67.

Ausführung an. Wenn die Individuen im Voraus über die drohende Abhörung ihrer Korrespondenzen wissen, ist die Durchführung solcher Abhörmaßnahmen etwa als Ermittlungsmaßnahme für die staatlichen Geheimdienste kaum erfolgsversprechend. In Kenntnis dieser Interessenlage und der Funktion der Telekommunikationsabhörung hat der EGMR das Kriterium der Vorhersehbarkeit für den spezifischen Fall der geheimdienstlichen Telekommunikationsausspähung folgendermaßen verstanden:

> „The Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly“.[381]

Folglich muss das Gesetz nicht insoweit bestimmt sein, dass im Einzelfall Individuen aus dem Gesetz konkret die Überwachung ihrer Korrespondenz erkennen können. Allerdings weist der Gerichtshof anschließend darauf hin, dass gerade hinsichtlich staatlicher Maßnahmen, die geheim ausgeführt werden, ein erhöhtes Risiko willkürlicher Eingriffe besteht.[382] Insofern ist es unerlässlich, dass klare und detaillierte Regeln für die Telekommunikationsüberwachung in den einschlägigen Gesetzen niedergelegt sind. Dies untermauert der Gerichtshof mit einem Verweis auf die hochentwickelte Telekommunikationstechnologie in der modernen Welt.[383] Auch der Menschenrechtsausschuss hat in einigen *Concluding Observations* darauf hingewiesen, dass Gesetze über Telekommunikationsüberwachung bestimmte Anforderungen für eine ausreichende Bestimmtheit erfüllen müssen.[384] Das Individuum muss aus dem Gesetz die Kriterien für die Anordnung einer Telekommunikationsüberwachung entnehmen können. Hinsichtlich der einzelnen Voraussetzungen, die für eine hinreichende Bestimmtheit und Vorhersehbarkeit der gesetzlichen Grundlage im Sinne der Art. 17 IPbpR und Art. 8 EMRK gelten, ist die Jurisprudenz beider Spruchkörper sehr ähnlich. Die Spruchpraxis des EGMR ist jedoch umfangreicher. Einzelne Kriterien, die nach Ansicht beider Spruchkörper für die Beurteilung der

---

[381] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 93; dazu grundlegend bereits *Malone v. The United Kingdom,* Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 67 und *Leander v. Sweden,* Rs. 9248/81, 26. März 1987, Series A116, Rn. 51. Vgl. auch EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 333.

[382] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 93; außerdem *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 67.

[383] EGMR, *Kopp v. Switzerland*, Rs. 23224/94, 25. März 1998, Rep. 1998-II, Rn. 72; *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 93.

[384] UN Human Rights Committee, Concluding observations: Russian Federation, CCPR/C/79/Add. 54, 26. Juli 1995, Rn. 19; Concluding observations: Jamaica, CCPR/C/79/Add. 83, 19. November 1997, Rn. 20.

hinreichenden Bestimmtheit der Überwachungsgesetze erheblich sind, werden nachfolgend dargelegt.[385]

aa. Zuständige Behörden

Die Behörden, die für die Durchführung von Maßnahmen zur Telekommunikationsausspähung zuständig sind, müssen im Gesetz klar benannt sein.[386] Der EGMR hat dabei klargestellt, dass es den Staaten zwar zustehe, den zuständigen Behörden einen Ermessenspielraum zu gewähren.[387] Die Grenzen des Ermessensspielraums und die konkreten Befugnisse der zuständigen Behörden müssen jedoch deutlich in dem Gesetz niedergelegt sein, um Individuen vor willkürlichen Eingriffen zu schützen.[388]

bb. Überwachungsbegründende Handlungen

Das Gesetz muss definieren, welche Art von Handlungen, die staatliche Interessen potenziell gefährden, die Anordnung von Überwachungsmaßnahmen begründen können.[389] Das zugrundeliegende Gesetz darf demnach nicht offen lassen, wann die zuständigen Behörden Überwachungsmaßnahmen anordnen können. Dabei sind

---

[385] Der EGMR prüft in Überwachungsfällen regelmäßig im Rahmen der Bestimmtheit der Gesetze die Bestimmtheit des Gesetzes und die Verhältnismäßigkeit zusammen. Siehe dazu die Ausführungen des Gerichtshofs in EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 334. Grundsätzlich prüft der EGMR dabei folgende sechs Mindestanforderungen: „[...](i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed", EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 335. Siehe dazu auch *Murray,* Practitioners' Guide to Human Rights Law in Armed Conflict, S. 312. Im Fall *Big Brother Watch and Others v. The United Kingdom* legt er wiederum dar, dass in Fällen der Massenüberwachung weitere Kriterien für die Beurteilung der Bestimmtheit und Verhältnismäßigkeit hinzuzuziehen sind. Siehe dazu den folgenden Unterabschnitt B. II. 5. B. b. bb.

[386] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 8; UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.7.

[387] EGMR, *Malone v. The United Kingdom,* Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 68.

[388] Ebd., Rn. 68; *M.M. v. The United Kingdom,* Rs. 24029/07, 13. November 2012, Rn. 193; *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 95; ebenso zuletzt in *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 333.

[389] Siehe dazu etwa UN Human Rights Committee, Concluding observations: Norway, CCPR/C/NOR/CO/7, 25. April 2018, Rn. 21; Concluding observations: Denmark, CCPR/C/DNK/CO/6, 15. August 2016, Rn. 28; Concluding observations: Rwanda, CCPR/C/RWA/CO/4, 2. Mai 2016, Rn. 36. Außerdem UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.7.

die Staaten jedoch nicht verpflichtet, eine umfassende namentliche Aufzählung aller Verhaltensweisen und Umstände, die eine Überwachung nach sich ziehen können, in den Gesetzen detailliert niederzulegen.[390] Verhaltensweisen, die etwa für die nationale Sicherheit gefährlich sein können, sind für den Gesetzgeber nämlich nicht immer vorhersehbar. In diesem Sinne führte der EGMR in der Entscheidung *Kennedy v. The United Kingdom* folgendes aus:

> „The Court has previously emphasised that the requirement of ‚foreseeability' of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on ‚national security' grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance […]. Similar considerations apply to the use of the term in the context of secret surveillance."[391]

In Überwachungsgesetzen kann es mithin genügen, wenn die einschlägigen Bestimmungen Überwachungsmaßnahmen für Aktivitäten anordnen, die eine „Bedrohung für die nationale Sicherheit" darstellen können. Dabei kommt es jedoch darauf an, ob beispielsweise die Rechtspraxis in ausreichendem Maße konkretisiert, wann von einer Bedrohungslage für die staatliche Sicherheit auszugehen ist.[392] In der Entscheidung *Centrum för rättvisa v. Sweden*[393] hat der Gerichtshof die hinreichende Bestimmtheit des schwedischen Gesetzes über die Fernmeldeaufklärung[394] geprüft. Nach Abschnitt 1 (2) dieses Gesetz dürfen Überwachungsmaßnahmen nur bei Vorliegen von acht ausdrücklich aufgezählten Gründen angeordnet werden.[395] Unter anderem werden hier militärische Bedrohungen für den Staat, strategische Erwägungen aufgrund des internationalen Terrorismus oder anderer grenzüberschreitender Verbrechen sowie ausländische Einwirkungen auf die schwedische Außen-, Sicherheits- oder Verteidigungspolitik als Gründe genannt.[396] Die im Gesetz

[390] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 159; *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 64.
[391] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 159.
[392] Vgl. die Argumentation des EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 369.
[393] EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021.
[394] Das „*Lagen om signalspaning i försvarsunderrättelseverksamhet*" ist 2009 erlassen worden und ist die schwedische Gesetzesgrundlage für Überwachungsmaßnahmen, siehe EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 17.
[395] Ebd., Rn. 284.
[396] Ebd., Rn. 284: „As noted by the Chamber, according to the Signals Intelligence Act signals intelligence may be conducted only to monitor: 1. external military threats to the country; 2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations; 3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national

benannten Überwachungsgründe sind dabei knapp formuliert. Dennoch geben sie zu erkennen, zu welchen Zwecken die Überwachung angeordnet werden kann und schließen eine grundlose Überwachung aus. Der EGMR verweist in seinem Urteil auf die Erläuterungen des Gesetzes, die die gesetzlich aufgezählten Überwachungsgründe beschreiben und definieren.[397] Der Gerichtshof bejaht deswegen die hinreichende Bestimmung der überwachungsbegründenden Handlungen und Umstände im schwedischen Überwachungsgesetz.[398]

cc. Zu überwachende Personen

Wichtig ist zudem, dass der Personenkreis, dessen Telekommunikation aufgrund des Gesetzes überwacht werden kann, in dem Gesetz benannt wird.[399] Dieses Kriterium kann indes mit der Definition der überwachungsbegründenden Umstände, die Anlass zur Überwachung geben, zusammenhängen. Denn die Definition der Handlungen, die Überwachungsmaßnahmen auslösen, grenzt auch den betroffenen Personenkreis auf eben jene ein, die zumindest verdächtig sind, Verursacher dieser Handlungen zu sein. Diese Überschneidung stellte der EGMR etwa im Fall *Kennedy v. The United Kingdom* fest:

> „In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception […] give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted.“[400]

Diese Überschneidung tritt jedoch nur auf, wenn das Gesetz ausdrücklich nur für solche Personen Überwachungsmaßnahmen vorsieht, die im Verdacht stehen, Täter der beschriebenen Handlungen zu sein. Häufig sind Überwachungsgesetze allerdings nicht auf verdächtige Personen begrenzt, sondern sehen zwecks effektiver Informationsgewinnung auch die Ausspähung der Telekommunikation von Dritten

interests; 4. the development and proliferation of weapons of mass destruction, military equipment and other similar specified products; 5. serious external threats to society's infrastructure; 6. foreign conflicts with consequences for international security; 7. foreign intelligence operations against Swedish interests; and 8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy".

[397] EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 22, 285.

[398] Ebd., Rn. 285 ff.

[399] Der MRA hat dieses Kriterium in einer Reihe von *Concluding Observations* genannt, siehe beispielsweise UN Human Rights Committee, Concluding observations: Norway, CCPR/C/NOR/CO/7, 25. April 2018, Rn. 21; Concluding observations: Lebanon, CCPR/C/LBN/CO/3, 9. Mai 2018, Rn. 34; Concluding observations: Rwanda, CCPR/C/RWA/CO/4, 2. Mai 2016, Rn. 36; Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12; Concluding observations: USA, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22.

[400] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 160; siehe außerdem *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 66.

vor, die beispielsweise mit Verdächtigen in Kontakt standen. In diesen Fällen würde es sich um eine gezielte Überwachung handeln, in der die zu überwachenden Personen im Voraus zumindest weitgehend feststehen. Nur Verdächtige und beispielsweise deren Kontaktpersonen wären das Ziel der Überwachungsmaßnahmen. Die Definition der Straftaten kann somit im Einzelfall als Indiz für die Beurteilung der hinreichenden Bestimmung des betroffenen Personenkreises berücksichtigt werden, sie kann aber keineswegs immer den vom Gesetz betroffenen Personenkreis hinreichend definieren.

Geheimdienstliche Überwachungsgesetze sind bisweilen auch deutlich weitgehender gefasst und erfassen potenziell einen erheblichen Teil der gesamten Bevölkerung eines Staates. Solche Gesetze autorisieren letztendlich häufig eine undifferenzierte Massenspionage.[401] Eine Definition des Personenkreises ist entweder gar nicht oder nur sehr allgemein vorgesehen. Ob solche gesetzlich vorgesehenen Massenüberwachungen das Kriterium der gesetzlichen Personenbestimmung erfüllen, kann zweifelhaft sein.[402] Streng genommen erfolgt keine gesetzliche Bestimmung des betroffenen Personenkreises und die gesetzliche Regelung sieht die Überwachung aller Individuen im Staat vor. Ob solche Gesetze mit Art. 8 EMRK und Art. 17 IPbpR vereinbar sind, wird in einem folgenden Unterabschnitt untersucht.

dd. Dauer der Überwachung

Auch die Dauer der Überwachungsmaßnahmen muss im Gesetz geregelt sein. Das Gesetz darf in diesem Sinne keine unbegrenzte Überwachung zugrunde legen, sondern muss vielmehr eine zeitliche Begrenzung vorsehen.[403] Dabei ist eine Verlängerung der zunächst festgesetzten Dauer der Überwachung nicht ausgeschlossen, solange das Gesetz die Voraussetzungen und das Verfahren der Verlängerung der Überwachungsanordnung in aller Klarheit definiert.[404] Damit soll ein Machtmissbrauch der Überwachungsorgane verhindert werden. In entsprechenden Entscheidungen hat der EGMR etwa die Verpflichtung von staatlichen Überwachungsorganen zur Beendigung der Überwachung in Fällen der Zielerreichung oder anderer Gründe, die eine Fortführung der Maßnahmen unnötig machen, positiv hervorgehoben. Solche Regulierungen würden in der Praxis eine regelmäßige Überprüfung der laufenden Überwachungsmaßnahmen und ihrer Anordnungsgrundlagen zur Folge haben.[405]

---

[401] Siehe dazu Ebd., Rn. 67 ff.
[402] Zur Rechtmäßigkeit der Massenüberwachung siehe 2. Abschnitt, Unterabschnitt B. II. 5.
[403] UN Human Rights Committee, Concluding observations: USA, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22.
[404] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 161; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 250.
[405] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 161; EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 401.

ee. Das Verfahren zur Verarbeitung, Weitergabe und Löschung der erlangten Daten

Das Gesetz muss zudem ausdrücklich niederlegen, wie mit den ausgespähten Daten nach ihrer Erlangung durch die zuständigen Behörden umgegangen wird. Denn angesichts der in Art. 17 IPbpR und Art. 8 EMRK verankerten Datenschutzgrundsätze müssen in den nationalen Überwachungsgesetzen Regelungen über die Verarbeitung, Herausgabe und Löschung der gewonnenen Telekommunikationsdaten enthalten sein, die mit diesen Grundsätzen im Einklang stehen.[406] Damit soll insbesondere die Gefahr reduziert werden, dass die vertraulichen Telekommunikationsdaten öffentlich enthüllt oder in die Hände von Unbefugten geraten.[407]

Ausführliche Regelungen zur Speicherung, Auswertung, Verwendung sowie sonstiger Verarbeitung der erlangten Telekommunikationsdaten müssen in den Gesetzen enthalten sein.[408] Der EGMR hat in diesem Sinne etwa Vorschriften zur sicheren Speicherung der Daten, die vor unberechtigten Zugriffen schützen,[409] sowie klare Speicherungsfristen in den Gesetzen[410] hervorgehoben. Weiterhin sind explizite Anordnungen über die Verfahrensweise der Auswertung von den ausgespähten Daten sowie eine zeitliche sowie personelle Begrenzung der Datenanalyse für die Beurteilung der hinreichenden Bestimmtheit der Gesetze von Bedeutung.[411] Auch die gesetzliche Regulierung der Festlegung und Anwendung von Suchbegriffen zur gezielten Analyse des Datenmaterials spielen eine wichtige Rolle.[412]

Zudem müssen klare Vorschriften und Vorkehrungen die Übermittlung der Daten an Dritte, wie etwa an andere Behörden oder auch an andere Staaten, regeln.[413] Zum Schutz der personenbezogenen Daten sollten nur solche Personen Zugang zu den Daten erhalten dürfen, die aufgrund von spezifischen Prüfungsverfahren

---

[406] So verweist auch der EGMR an entsprechender Stelle auf die in der europäischen Datenschutzkonvention verankerten Datenschutzgrundsätze, siehe EGMR, *M.M. v. The United Kingdom*, Rs. 24029/07, 13. November 2012, Rn. 196.

[407] EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 253. Siehe auch die Argumentation des EGMR im Fall *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 163.

[408] EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 56.

[409] So etwa in EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 390.

[410] Siehe dazu beispielsweise EGMR, *Rotaru v. Romania* [GC], Rs. 28341/95, 4. Mai 2000, Rep. 2000-V, Rn. 57. Hier kritisiert der EGMR, dass die rumänischen Gesetze, die die Grundlage für geheimdienstliche Überwachungsmaßnahmen bilden, keine zeitliche Begrenzung zur Aufbewahrung von Daten haben.

[411] Vgl. Argumentation des EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 384 ff.

[412] Siehe dazu EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 32.

[413] Siehe etwa Ebd., Rn. 99; Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 27.

offiziell die Befugnis hierzu erhalten haben.[414] Letztlich wird hiermit sichergestellt, dass die dritte Person darin geschult ist, mit den erhaltenen Daten entsprechend der datenschutzrechtlichen Grundsätze umzugehen. Des Weiteren sollten die befugten Personen nur diejenigen Daten erhalten, die für die von Ihnen verfolgten legitimen Ziele tatsächlich notwendig sind.[415] Eine im Gesetz vorgesehene undifferenzierte Weitergabe von jeglichen Daten an Dritte wäre mit dem Grundsatz der Bestimmtheit des Gesetzes unvereinbar.[416]

Schließlich muss ausdrücklich geregelt sein, unter welchen Umständen die Daten gelöscht und vernichtet werden müssen. So hat der EGMR etwa in einschlägigen Fällen hervorgehoben, dass die zugrundeliegenden Gesetze die sofortige Löschung von Daten anordnen sollten, die keinen Bezug zu dem mit der Überwachung verfolgten Ziel haben[417] oder der sachliche Bezug nicht mehr fortbesteht.[418] Auch im Rahmen von Strafverfahren, in denen letztlich die angeklagten Individuen freigesprochen werden, müssen klare Verfahren zur Löschung von Telekommunikationsdaten, die zu Ermittlungszwecken ausgespäht wurden, reguliert sein.[419]

3. Legitimes Ziel der Telekommunikationsüberwachung

Staatliche Beschränkungen des Schutzes der Privatsphäre müssen einen legitimen, mit dem Menschenrechtspakt im Einklang stehenden Zweck verfolgen. Während Art. 8 Abs. 2 EMRK die legitimen Ziele für Beschränkungen des Art. 8 Abs. 1 EMRK ausdrücklich aufzählt, ist eine solche Auflistung in Art. 17 IPbpR nicht enthalten.

Nach Art. 8 Abs. 2 EMRK können die Vertragsstaaten das Recht auf Privatsphäre ausschließlich zum Zwecke der nationalen oder öffentlichen Sicherheit, des wirtschaftlichen Wohls des Landes, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten, des Schutzes der Gesundheit oder der Moral und schließlich des Schutzes der Rechte und Freiheiten anderer einschränken. Die Liste der legitimen Ziele ist somit weitgefächert und so stellt auch der EGMR in aller Regel

---

[414] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 390.

[415] Ebd.

[416] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 27.

[417] Siehe EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 255: „At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained [...]. The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8." Außerdem EGMR, *Klass and Others v. Germany*,
Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 52; *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008, Rn. 68; *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 162.

[418] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn 100.

[419] EGMR, *Kruslin v. France*, Rs. 11801/85, 24. April 1990, Serie A 176-A, Rn. 35.

fest, dass die staatlichen Beschränkungsmaßnahmen, die den Individualbeschwerden zugrunde liegen, eines der aufgezählten Ziele verfolgen.[420]

Auch Eingriffe in Art. 17 IPbpR müssen einem legitimen Zweck dienen.[421] Zwar gibt Art. 17 IPbpR nicht ausdrücklich vor, auf Grundlage welcher Ziele Beeinträchtigungen gerechtfertigt sein können. Allerdings kann aufgrund der Bedeutsamkeit des Schutzes der Privatsphäre davon ausgegangen werden, dass nicht jeder beliebige Zweck für eine Einschränkung des Art. 17 IPbpR herangezogen werden darf.[422] Eine Orientierung darüber, welche Ziele für einen Eingriff in den Schutz der Privatsphäre gemäß Art. 17 IPbpR möglich sind, liefern die Art. 12 Abs. 3, 18 Abs. 3 , 19 Abs. 3, 21 und 22 Abs. 2 IPbpR.[423] In diesen Artikeln werden die nationale Sicherheit, Öffentliche Ordnung (*ordre public*), Schutz der allgemeinen Gesundheit und Moral sowie der Schutz der Rechte und Freiheiten anderer als Eingriffsziele genannt und sind damit dem Katalog in Art. 8 EMRK sehr ähnlich.

In den Fällen der geheimdienstlichen Telekommunikationsausspähung steht die Wahrung der nationalen Sicherheit als Zweck gewiss im Vordergrund.[424] Die Staaten der heutigen Welt und ihre Geheimdienste stehen vor komplexeren Sicherheitsherausforderungen. Insbesondere stellt der moderne internationale Terrorismus die Effektivität aller bisherigen nationalen Mechanismen zum Schutz der nationalen Sicherheit in Frage. Wie unter dem Abschnitt der Funktion der geheimdienstlichen Spionage bereits ausgeführt, sind die dezentrale Organisation sowie die ideologische Motivation Hauptmerkmale dieser neuen Form des Terrorismus, die zu einer Unberechenbarkeit der gesamten Gefahrenlage führt.[425] Die globale Vernetzung der Terrororganisationen erschwert die Lokalisierung der Gefahrenquelle erheblich. Es lässt sich damit nicht ohne weiteres vorhersagen, woher der nächste Angriff kommen wird. Die Gefahrenquelle kann sich ebenso gut inmitten der eigenen Gesellschaft befinden. Dies kann insbesondere auch darauf beruhen, dass Individuen und Terrorzellen völlig autonom agieren oder motiviert durch große Terrornetzwerke eigenständig Attentate verüben.

Die Staaten stehen dabei heute vor der schwierigen Aufgabe, den komplexen Bedrohungen, die die Sicherheit ihrer Bürger gefährden, effektiv zu begegnen. Dieser Umstand erklärt auch das dringende Bedürfnis der Staaten, unter Anwendung

[420] Vgl. *Schabas,* The European Convention on Human Rights, Art. 8, S. 404.
[421] *Nowak*, CCPR Commentary, Art. 17, S. 382–383, Rn. 12–13; UN Human Rights Committee, Concluding observations: Lebanon, CCPR/C/LBN/CO/3, 9. Mai 2018, Rn. 34.
[422] *Nowak*, CCPR Commentary, Art. 17, S. 383, Rn. 13.
[423] Ebd.
[424] Siehe etwa EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232. Vgl. außerdem Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 24.
[425] 1. Abschnitt, Unterabschnitt B. II.

modernster Formen der Telekommunikationsüberwachung einzelne Individuen und Gruppierungen als Gefahrenquellen ausfindig zu machen.[426]

Dabei sei an dieser Stelle darauf hingewiesen, dass der EGMR entsprechend seiner „*margin of appreciation*"-Rechtsprechung den Staaten für Maßnahmen zum Schutz der nationalen Sicherheit einen grundsätzlich weiten Ermessensspielraum einräumt.[427] Wie bereits dargelegt, hebt der EGMR auch im Kontext der Telekommunikationsüberwachung regelmäßig hervor, dass den Vertragsstaaten grundsätzlich ein weiter Beurteilungsspielraum zukommt.[428] Dennoch äußert sich auch der EGMR regelmäßig an gegebener Stelle zu den Hintergründen der staatlichen Überwachungsmaßnahmen.[429] Hieraus wird deutlich, dass der Gerichtshof die Hintergründe der Überwachungsmaßnahmen der Staaten trotz des eingeräumten Beurteilungsspielraums durchaus in seiner Entscheidungsfindung einbezieht.

Der MRA räumt den Staaten hingegen einen deutlich engeren Entscheidungsspielraum ein. Nach Ansicht des Ausschusses kann den Vertragsstaaten auch in Fragen der nationalen Sicherheit kein uneingeschränktes Ermessen überlassen werden. So unterliegen demnach auch staatliche Erwägungen für die nationale Sicherheit der Kontrolle des Ausschusses.[430] Der MRA hat in diesem Sinne im Bereich des nationalen Strafrechts grundsätzlich festgestellt, dass die Ausspähung von Telekommunikationsdaten grundsätzlich nicht für Bagatelldelikte angewendet werden sollte, sondern auf die Bekämpfung schwerer Kriminalität zu begrenzen sei.[431]

---

[426] Vgl. auch EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 48. Außerdem Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 24.

[427] *Asche,* Die Margin of Appreciation, S. 73.

[428] EGMR, *Leander v. Sweden*, Rs. 9248/81, 26. März 1987, Series A116, Rn. 59; *Dragojević v. Croatia*, Rs. 68955/11, 15. Januar 2015, Rn. 84; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232; *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 338 f.

[429] Siehe beispielsweise EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 68.

[430] Vgl. Human Rights Committee, *Vjatseslav Borzov v. Estonia,* No. 1136/2002, CCPR/C/81/D/1136/2002, 25. August 2004, Rn. 7.3: „While the Committee recognizes that the Covenant explicitly permits, in certain circumstances, considerations of national security to be invoked as a justification for certain actions on the part of a State party, the Committee emphasizes that invocation of national security on the part of a State party does not, ipso facto, remove an issue wholly from the Committee's scrutiny.[...] While the Committee cannot leave it to the unfettered discretion of a State party whether reasons related to national security existed in an individual case, it recognizes that its own role in reviewing the existence and relevance of such considerations will depend on the circumstances of the case and the relevant provision of the Covenant." Siehe dazu außerdem *McGoldrick,* A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee, S. 55 f.

[431] UN Human Rights Committee, Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 29, 30.

Weitere Ziele, die mit der Telekommunikationsüberwachung angestrebt werden können, sind etwa Kriminalitätsbekämpfung im Allgemeinen[432] oder auch die Wahrung des wirtschaftlichen Wohls des Staates sein.[433]

Der Zweck der konkreten Überwachungsmaßnahme muss freilich auch in der Interessenabwägung für die Untersuchung der Verhältnismäßigkeit angemessen gewichtet werden. Denn letztlich steht die Frage im Raum, ob der Eingriff in Form der Telekommunikationsüberwachung angesichts des konkreten Zwecks verhältnismäßig ist. Dies hängt auch von der Bedeutsamkeit des verfolgten Zwecks ab.

4. Verhältnismäßigkeit der Telekommunikationsüberwachung

Sind die strengen Voraussetzungen der gesetzlichen Grundlage erfüllt und verfolgt die geheimdienstliche Telekommunikationsüberwachung einen legitimen Zweck, so muss anschließend für eine Rechtfertigung der Überwachung das wichtige Kriterium der Verhältnismäßigkeit erfüllt sein. Die „Verhältnismäßigkeit" wird begrifflich zwar weder in Art. 8 EMRK noch Art. 17 IPbpR ausdrücklich genannt. Allerdings ist dieses Prinzip in beiden Artikeln als zentrales Kriterium einer Rechtfertigung von Eingriffen in das Menschenrecht auf Privatsphäre niedergelegt. Grundlage des Verhältnismäßigkeitsprinzips in Art. 17 IPbpR ist die Formulierung „*arbitrary interference*". Das Verbot willkürlicher Eingriffe in Art. 17 IPbpR soll gewährleisten, dass auch gesetzlich vorgesehene Eingriffe nicht unbegrenzt das Recht auf Privatsphäre einschränken können.[434] So muss der Eingriff im Verhältnis zum angestrebten Ziel notwendig und verhältnismäßig sein:

> „As to whether it may be deemed arbitrary, the Committee recalls that pursuant to its general comment 16 (32) on article 17, the ‚introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by the law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the circumstances'. The Committee interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[435]

[432] EGMR, *Kennedy v. The United Kingdom,* Rs. 26839/05, 18. Mai 2010, Rn. 155; UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.10.

[433] EGMR, *Kennedy v. The United Kingdom,* Rs. 26839/05, 18. Mai 2010, Rn. 155.

[434] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 4.

[435] UN Human Rights Committee, *Toonen v. Australia*, No. 488/1992, CCPR/C/50/D/488/1992, 31. März 1994, Rn. 8.3. Siehe außerdem *Nowak*, CCPR Commentary, Art. 17, S. 383, Rn. 12; *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 16.10. Der Begriff „*arbitrary*"

Gemäß Art. 8 Abs. 2 EMRK müssen Eingriffe in das Recht auf Privatsphäre „in einer demokratischen Gesellschaft notwendig" sein („*necessary in a democratic society*"). In seiner ständigen Rechtsprechung hat der EGMR zur Auslegung des Begriffes „Notwendigkeit" festgestellt, dass ein Eingriff einerseits einem dringenden gesellschaftlichen Bedürfnis dienen und zudem verhältnismäßig zum angestrebten Ziel sein muss.[436]

Schwerpunkt der Verhältnismäßigkeitsprüfung in der Judikatur des MRA und des EGMR ist zweifelsfrei die Interessenabwägung im Rahmen der Angemessenheit. Der EGMR nimmt in seiner Argumentation regelmäßig keine strenge Trennung zwischen der Geeignetheit, der Erforderlichkeit und der Angemessenheit vor. Ausführungen insbesondere zu Fragen der Geeignetheit, aber auch zur Erforderlichkeit, sind in seiner Judikatur allenfalls knapp. Dies beruht insbesondere auch auf der „*margin of appreciation*"-Doktrin des Gerichtshofs, wonach die Staaten hinsichtlich der Auswahl ihrer Maßnahmen zur Erreichung des legitimen Zwecks einen weiten Beurteilungsspielraum haben.[437] So hat der EGMR auch für Fälle der Telekommunikationsüberwachung die „*margin of appreciation*"-Doktrin ausdrücklich angewendet. Dabei räumt der Gerichtshof den Staaten prinzipiell einen weiten Beurteilungsspielraum hinsichtlich ihrer Maßnahmen zur Telekommunikationsüberwachung ein, wobei dieser Beurteilungsspielraum dennoch der Aufsicht des EGMR unterliegt.[438] Hingegen führt der MRA in seinen *Views* mitunter auch umfassende Erforderlichkeitsprüfungen durch und verneint die Verhältnismäßigkeit von einzelnen Maßnahmen aufgrund milderen zur Verfügung stehenden Eingriffsmitteln.[439]

---

bezieht sich indes auf die in Art. 17 IPbpR aufgelisteten Schutzgüter mit Ausnahme des Schutzes der Ehre und des guten Rufes. Hierfür gilt allein das Kiterium „*lawful*".

[436] Vgl. EGMR*, S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008, Rn. 101; *Uzun v Germany*, Rs. 35623/05, 2. September 2010, Rn. 78.

[437] Siehe dazu grundlegend EGMR, *Handyside v. The United Kingdom,* Rs. 5493/72, 07. Dezember 1976, Serie A 24, Rn. 48 f. Siehe außerdem EGMR, *Leander v. Sweden,* Rs. 9248/81, 26. März 1987, Series A116, Rn. 59; Weber *and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 106; *Dragojević v. Croatia,* Rs. 68955/11, 15. Januar 2015, Rn. 84. Zum Thema der „*margin of appreciation*"-Doktrin des EGMR *Asche,* Die Margin of Appreciation.

[438] Vgl. etwa EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, 154; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232; *Dragojević v. Croatia*, Rs. 68955/11, 15. Januar 2015, Rn. 84.

[439] Sehr deutlich erkennbar ist dies etwa in der Entscheidung UN Human Rights Committee, *Keun-Tae Kim v. Republic of Korea,* No. 574/1994, CCPR/C/64/D/574/1994, 3. November 1998, Rn. 12.4. Vgl. auch *Omar Sharif Baban v. Australia*, No. 1014/2001, CCPR/C/78/D/1014/2001, 6. August 2003, Rn. 7.2. Siehe dazu auch *Von Bernstrorff,* Kerngehaltsschutz durch den UN-Menschenrechtsausschuss und den EGMR, S.180. Der MRA lehnt die Anwendung einer „*margin of appreciation*"-Doktrin in seiner Jurisprudenz ausdrücklich ab, vgl. etwa UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of opinion and expression), CCPR/C/GC/34, 12. September 2011, Rn. 36: „The Committee reserves to itself an assessment of whether, in a given situation, there may have been circumstances which made a restriction of freedom of expression necessary. In this regard, the Committee recalls that the scope of this freedom is not to be assessed by reference to a ‚margin of appreciation' and in order for the Committee to carry out this function, a State party,

Auch geheimdienstliche Überwachungsmaßnahmen müssen im Einzelfall die Anforderungen der Geeignetheit und Erforderlichkeit erfüllen. Grundsätzlich sind gezielte Überwachungsmaßnahmen dazu geeignet, einzelne Gefahrenquellen beispielsweise für die nationale Sicherheit zu identifizieren. Die hierauf folgende Eindämmung dieser Gefahrenquellen – gerade in Hinsicht auf mutmaßliche Terroristen – würde die nationale Sicherheit fördern. Mildere Mittel im Sinne des Kriteriums der Erforderlichkeit wären keineswegs ausgeschlossen. Dazu müsste in Abhängigkeit der Reichweite und Intensität der konkret angeordneten Überwachungsmaßnahmen ermittelt werden, welche anderen Ermittlungsmethoden als mildere Maßnahmen in Frage kämen. Kritischer Punkt wäre dann jedoch, ob die gleiche Wirksamkeit erzielt wird. Generell ist eher damit zu rechnen, dass gerade gezielte Maßnahmen der modernen Telekommunikationsüberwachung eine Fülle von ermittlungsrelevanten Informationen in kürzester Zeit bereitstellen können. Es kann mithin nicht ohne Weiteres davon ausgegangen werden, dass andere Ermittlungsmaßnahmen eine vergleichbare Effektivität erzielen.

Im Rahmen der Angemessenheit ist eine Abwägung der widerstreitenden Interessen vorzunehmen. Im Fall der Telekommunikationsüberwachung steht einerseits das Menschenrecht auf Privatsphäre, und zwar konkret der Schutz der Vertraulichkeit der Korrespondenz und der personenbezogenen Daten, im Raum. Die Überwachung betrifft dabei den sensiblen Bereich des privaten Informationsaustausches, der für betroffene Individuen, die innerhalb eines gesellschaftlichen Sozialgefüges leben und agieren, von fundamentaler Bedeutung ist. Andererseits sind die staatlichen Interessen, die solchen Telekommunikationsüberwachungsprogrammen zugrunde liegen, von hohem Stellenwert. So dienen etwa nationale Sicherheit und Kriminalitätsbekämpfung dem Wohl der Allgemeinheit. Somit stehen hier auf beiden Seiten wichtige und schützenswerte Interessen gegenüber.

Der EGMR hebt im Zusammenhang dieser Fälle regelmäßig hervor, dass ein System geheimer Telekommunikationsausspähung die Demokratie unterminieren oder gar zerstören könne.[440] Tatsächlich erfordert die Interessenabwägung im Kontext geheimer Überwachungsmaßnahmen aufgrund der hohen Missbrauchsgefahr ein Höchstmaß an Sorgfalt. So muss den prinzipiell berechtigten Interessen des Staates Rechnung getragen werden, ohne das Menschenrecht auf Privatsphäre auszuhöhlen. Diese Kollision kann nur unter Berücksichtigung der konkreten Umstände des Einzelfalles von Fall zu Fall aufgelöst werden. Dies entspricht auch der Herangehensweise des EGMR sowie des UN-Menschenrechtsausschusses. In der Spruchpraxis beider Spruchkörper haben sich in diesem Sinne Kriterien etabliert, die für eine menschenrechtskonforme Interessenabwägung berücksichtigt und

in any given case, must demonstrate in specific fashion the precise nature of the threat to any of the enumerated grounds listed in paragraph 3 that has caused it to restrict freedom of expression." Siehe zu diesem Thema ausführlich: *McGoldrick,* A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee.

[440] Vgl etwa EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 57.

ausgewertet werden müssen. So muss neben der Bedeutsamkeit des konkreten Zwecks der Überwachung im Einzelfall zudem insbesondere die Eingriffsintensität bewertet werden. Art, Dauer und Umfang der Überwachung sind in diesem Zusammenhang wichtige Indizien. Darüber hinaus hängt die Frage nach der Verhältnismäßigkeit der konkreten Maßnahme insbesondere auch vom staatlichen Verfahren der Genehmigung und Aufsicht der Telekommunikationsüberwachung sowie dem Vorhandensein effektiver Rechtsmittel für betroffene Individuen ab.

a. Die Eingriffsintensität der Überwachungsmaßnahmen

Im Vergleich zu anderen Formen der Überwachung ist im Fall der Telekommunikationsüberwachung prinzipiell von einer hohen Eingriffsintensität auszugehen.[441] Denn die Mittel der Telekommunikation werden von den betroffenen Individuen für private Korrespondenz unter Ausschluss der Öffentlichkeit genutzt. Dabei werden persönliche Meinungen, Emotionen oder andere intime Informationen ausgetauscht.[442] Durch die geheime Abhörung ist folglich ein sensibler Bereich des Menschenrechts auf Privatsphäre berührt. Diese Form der Überwachung tangiert nicht nur den Schutz der Korrespondenz, sondern stellt auch einen Eingriff in den Schutz der personenbezogenen Daten.[443] Somit sind bei dieser Überwachungsform mehrere Schutzgüter aus Art. 17 IPbpR sowie Art. 8 EMRK betroffen.[444]

Aber auch innerhalb dieser verhältnismäßig hohen Intensität der Telekommunikationsausspähung gibt es Abstufungen. So ist nicht grundsätzlich jede Telekommunikationsüberwachung per se aufgrund ihrer hohen Eingriffsintensität menschenrechtswidrig. Vielmehr gewähren Art. 17 IPbpR sowie Art. 8 EMRK Raum für die Rechtfertigung dieser intensiven Überwachungsmaßnahmen. Dabei ist jedoch die konkrete Intensität im Einzelfall ausschlaggebend. So können einige Faktoren die Intensität des Eingriffs maßgeblich erhöhen. Dabei spielen für die Beurteilung der Eingriffsintensität insbesondere die konkrete Art der staatlichen Telekommunikationsüberwachung, der gesamte Umfang der Überwachungsmaßnahmen sowie auch die Dauer der Ausspähung eine bedeutende Rolle. Die einzelnen Kriterien, die in diesem Rahmen intensivierend wirken können, werden im Folgenden anhand der einschlägigen Spruchpraxis ausgearbeitet.

---

441 Siehe etwa EGMR, *Uzun v Germany,* Rs. 35623/05, 2. September 2010, Rn. 66: „[The Court] finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications […], are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations“. Vgl. auch *R.E. v. The United Kingdom,* Rs 62498/11, 27. Oktober 2015, Rn. 131. Hier stellt der Gerichtshof indes überzeugend fest, dass die Abhörung der Rechtsberatung eines Anwalts an einen angeklagten Inhaftierten innerhalb einer Polizeistation ebenso intensiv ist, wie die Überwachung der Telefonkorrespondenz zwischen den beiden Personen.

442 EGMR, *Uzun v Germany,* Rs. 35623/05, 2. September 2010, Rn. 52.

443 Siehe oben 2. Abschnitt, Unterabschnitt B. I.

444 Siehe auch *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 149.

aa. Art, Umfang und Dauer der Telekommunikationsüberwachung

Die Gesamtheit aller Umstände, insbesondere Art, Umfang und Dauer der Telekommunikationsüberwachung, bestimmen die Intensität der konkreten Eingriffsmaßnahme.[445] So gibt letztlich eine umfassende Gesamtbetrachtung der Konstellation und der Zusammenwirkung all dieser Kriterien im Einzelfall Aufschluss über die verhältnismäßig geringere oder erhöhte Eingriffsintensität. Die Bandbreite der geheimdienstlichen Eingriffsmöglichkeiten ist dabei aufgrund der modernen Kommunikations- und Informationstechnologie sehr weit. So können die Geheimdienste unterschiedliche Arten der Telekommunikationsüberwachung anwenden und dabei mit technisch relativ geringem Aufwand den Umfang und die Dauer der Maßnahmen an ihre Ausspähungsziele beliebig anpassen.

Der Umfang der Überwachung richtet sich zunächst danach, ob Korrespondenzinhalte oder -metadaten ausgespäht werden oder ob im Rahmen einer Maßnahme beide Datentypen der einzelnen Korrespondenzen zeitgleich erfasst werden. Dies geschah etwa beim britischen Programm „*TEMPORA*“, das Korrespondenzinhalte sowie die entsprechenden Metadaten abfing.[446]

Die Inhaltsüberwachung gibt den Geheimdiensten Einblick in den inhaltlichen Gegenstand des privaten Dialogs. Damit werden direkt Informationen über private Absichten, Denkweisen und Emotionen gewonnen. Dahingegen umfasst eine reine Analyse der Telekommunikations-Metadaten nur äußere Informationen der Kommunikationsverbindung, etwa über den Zeitpunkt, den Ort und den Beteiligten der entsprechenden Korrespondenz. Jedoch ist die Metadaten-Ausspähung deswegen keineswegs per se weniger intensiv. Denn einerseits sind ebenso diese Telekommunikations-Metadaten auch von Art. 17 IPbpR sowie Art. 8 EMRK menschenrechtlich geschützt.[447] Insbesondere die systematische und langfristige Ausspähung solcher Metadaten kann Informationen über persönliche Verhaltensweisen, Beziehungen und Gewohnheitsmuster zutage fördern.[448] Damit ließe sich ein umfassendes persönliches und soziales Profil einer Person zusammenstellen. Werden etwa über einen längeren Zeitraum die Adressaten der Korrespondenzen einer Person erfasst, so ließe sich hieraus das soziale Netzwerk der betroffenen Person ohne größeren Aufwand ermitteln. Auch wenn letztlich keine Inhalte der einzelnen Korrespon-

[445] So auch der EGMR in seiner ständigen Rechtsprechung: EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 50; *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 153; *Dragojević v. Croatia*, Rs. 68955/11, 15. Januar 2015, Rn. 83; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232; *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 57.

[446] Dazu bereits 1. Abschnitt B. III. 2. A. Siehe außerdem EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 17.

[447] Siehe oben 2. Abschnitt, Unterabschnitte A. I. 2. c. und A. II. 2. b.

[448] So auch der Menschenrechtsrat in seiner Resolution zum Schutz der Privatsphäre im digitalen Zeitalter, UN Human Rights Council, Resolution 28/16 „The right to privacy in the digital age“, A/HRC/RES/28/16, 1. April 2015, S. 2. Siehe auch *Kittichaisaree*, Public International Law of Cyberspace, S. 66.

denzen bekannt werden, so ist in solchen systematischen und langfristigen Fällen der Metadaten-Ausspähung durchaus eine erhöhte Eingriffsintensität gegeben.[449] Eine parallele Überwachung beider Datentypen erhöht indes die Intensität des Eingriffs. Denn die Kombination offenbart den Behörden den vollständigen Datensatz einer Korrespondenz. Sowohl die Inhalte als auch die Verbindungsdaten wären in der Hand des Geheimdienstes.

Des Weiteren ist die Anzahl der von den Überwachungsmaßnahmen betroffenen Personen ein weiterer Faktor im Rahmen des gesamten Ausspähungsumfangs.[450] So kann sich die Überwachung der Telekommunikation gezielt gegen eine konkrete Einzelperson richten oder aber einen weiten Kreis von Personen betreffen. Dies hängt letztlich auch davon ab, ob die Überwachungsmaßnahme nur verdächtige Personen einbezieht oder verdachtsunabhängig ausgeführt wird. Eine verdachtsunabhängige Überwachung kann im Rahmen von Präventionsmaßnahmen Anwendung finden, die nicht an einen konkreten Verdacht anknüpfen. Dabei kann der Anwendungsradius solcher präventiven Überwachungsmaßnahmen in Fällen undifferenzierter und allgemeiner Ausspähung sehr weit sein.[451] Definieren die Sicherheitsbehörden im Vorfeld hingegen Suchbegriffe, die nur die für die konkreten Überwachungszwecke relevanten Informationen aus dem gesamten Pool an Korrespondenzdaten herausfiltern, so sind dementsprechend weniger Individuen von den Maßnahmen betroffen.[452] Die gesetzliche Grundlage der Telekommunikationsüberwachung muss hinsichtlich des betroffenen Personenkreises hinreichend bestimmt sein.[453] Je enger dabei die Definition des Personenkreises niedergelegt ist, umso geringer ist die Anzahl der betroffenen Personen. Für den Einzelnen wirkt sich eine fehlende Begrenzung des Personenkreises zwar nicht auf die Eingriffsintensität der Überwachung aus. Allerdings ist der weite Radius betroffener Personen durchaus in der Gesamtabwägung zu berücksichtigen. Dies kann nämlich die Anforderungen an die Schutzmaßnahmen und Rechtsbehelfe beeinflussen. Die Einzelheiten der Rechtfertigung von undifferenzierten und verdachtsunabhängigen

---

[449] So auch *Loideain,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, S. 54; *Paefgen,* Persönlichkeitsrechte im Internet*,* S. 144. Siehe dazu auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/ 27/37, 30. Juni 2014, Rn. 19.

[450] In der Rechtsprechung des EGMR ist die Anzahl der betroffenen Personen einerseits Prüfungsgegenstand der Bestimmtheit der gesetzlichen Grundlage. Außerdem bezieht der EGMR diesen Aspekt auch im Rahmen der Interessenabwägung gewichtend ein. Siehe etwa EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 66 ff.

[451] Vgl. auch Ebd., Rn. 67.

[452] Damit argumentierte auch der EGMR im Fall *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 97. So könne auf Grundlage des deutschen Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10) eine Überwachung angeordnet werden, sofern bestimmte Suchbegriffe in der Korrespondenz der Individuen genannt werden. Siehe dazu § 5 Abs. 2 des G-10-Gesetzes.

[453] Siehe 2. Abschnitt, Unterabschnitt B. II. 2. a. cc.

Massenüberwachungen werden gesondert dargestellt.[454] Die Anzahl der betroffenen Personen kann auch vom territorialen Anwendungsbereich der Telekommunikationsüberwachung abhängen. Eine extraterritoriale Korrespondenzüberwachung betrifft einen eklatant größeren Personenkreis als Überwachungsmaßnahmen, die auf das Inland begrenzt sind.[455]

Ein engriffsintensivierender Faktor kann darin bestehen, dass nicht hinsichtlich der Art der Korrespondenz unterschieden wird. So können durch Überwachungsmaßnahmen auch besonders schützenswerte Daten und Korrespondenzen – wie etwa sensible Korrespondenzen zwischen Anwalt und Mandanten, persönliche medizinische Auskünfte oder andere intime und sensible Informationen – unterschiedslos in das Netz der Geheimdienste fallen.[456] Dies könnte indes auch in andere Menschenrechte – neben dem Recht auf Privatsphäre – eingreifen. Im Fall *Big Brother Watch and Others v. The United Kingdom* machten die antragstellenden Journalisten auch eine Verletzung ihrer Rechte aus Art. 10 EMRK geltend.[457] Sie argumentierten damit, dass das entsprechende Überwachungsregime auch ihre journalistische Tätigkeit betreffe, da vertrauliches journalistisches Material in die Hände der Geheimdienste gelangen könne.[458]

Auch die Dauer der Überwachungsmaßnahmen kann im Einzelfall eingriffsintensivierend wirken. So ist sicherlich zwischen kurzen Ausspähungsmaßnahmen, die gezielt zur Ermittlung konkreter Informationen eingesetzt werden, und langzeitigen Überwachungssystemen zu unterschieden. Je länger der Zeitraum der Überwachung fortdauert, umso mehr personenbezogene Daten werden ermittelt. Im Fall einer Einzelfallüberwachung würden die über einen längeren Zeitraum erfassten Daten den Sicherheitsbehörden einen tieferen Einblick in die persönliche Sphäre der betroffenen Person ermöglichen. Damit lassen sich über einzelne Personen mit zunehmender Überwachungsdauer auch stetig detailliertere Persönlichkeitsprofile und Sozialkontexte erkennen. Hinsichtlich der Dauer der Überwachung ist zudem bedeutsam, ob und inwieweit Überwachungsmaßnahmen aufgrund der gesetzlichen Grundlagen verlängert werden können.

---

[454] Zur Massenüberwachung siehe nachfolgenden Unterabschnitt B. II. d.

[455] Zum Thema „extraterritoriale Telekommunikationsüberwachung" siehe 3. Abschnitt, Unterabschnitt A. II.

[456] So etwa im Fall EGMR, *R.E. v. The United Kingdom*, Rs 62498/11, 27. Oktober 2015, Rn. 131, in dem der EGMR die Überwachung einer anwaltlichen Beratung als einen Eingriff mit „extrem hoher Intensität" bezeichnet hat.

[457] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021.

[458] Im Ergebnis stellte der EGMR eine Verletzung von Art. 10 EMRK fest. Art. 8 (4) RIPA schreibe nach Ansicht des EGMR nämlich nicht vor, dass die Verwendung von Selektoren, von denen bekannt ist, dass sie mit einem Journalisten in Verbindung stehen, von einem unabhängigen Entscheidungsgremium genehmigt werden müsse. Des Weiteren seien keine Schutzmaßnahmen für den Fall vorgesehen, dass unabsichtlich vertrauliches journalistisches Material vom Geheimdienst aufgefangen wurde. Vgl. dazu EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 456 f.

Der Umfang und die Dauer der Überwachung müssen schließlich auch im breiteren Kontext der zugrundeliegenden Art der Telekommunikationsüberwachung betrachtet und gewichtet werden. Dabei geht es auch an dieser Stelle um die drei Hauptformen der modernen Telekommunikationsspionage, die im Fokus dieser Untersuchung stehen: Der direkte Zugriff auf das Telekommunikationsnetzwerk während der Datenübertragung, die Beschaffung von Telekommunikationsdaten aus Servern von *Service Providern* sowie der direkte Zugriff auf privatgenutzte Telekommunikationsgeräte.[459] Die Eingriffsintensität dieser Methoden der geheimdienstlichen Informationsgewinnung kann – auch in Abhängigkeit von Umfang und Dauer der konkreten Maßnahme – variieren.

(1) Zugriff auf das Telekommunikationsnetzwerk

Der direkte geheimdienstliche Zugriff auf das Telekommunikationsnetzwerk während der Datenübertragung ist eine moderne Abwandlung des klassischen „Abhörens". Hierbei werden allerdings nicht mehr einzelne Verbindungskabel angezapft, sondern vielmehr auf das globale Telekommunikationsnetzwerk zugegriffen, durch das permanent unzählige Verbindungsdaten fließen. Ein Beispiel hierfür ist das Überwachungsprogramm „*TEMPORA*" des britischen Geheimdienstes GCHQ, das Datenströme aus transatlantischen Glasfaserkabelverbindungen angezapft hat.[460] Ein weiteres Beispiel ist das vom US-Geheimdienst NSA operierte Programm „*UPSTREAM*".[461]

Diese moderne Form der Überwachung ist eher nicht dafür geeignet und in der Regel auch nicht darauf angelegt, Einzelkorrespondenzen aufzufangen. Vielmehr ist diese Form der Überwachung von vornherein breiter angelegt und betrifft in der Regel eine enorm hohe Anzahl von Personen. Für die Beurteilung der Eingriffsintensität dieser Form der Telekommunikationsüberwachung für das betroffene Individuum ist zu berücksichtigen, dass hierbei sowohl die Metadaten als auch Korrespondenzinhalte erfasst werden, wie dies etwa im Fall des britischen Überwachungsprogramms „*TEMPORA*" der Fall war. Des Weiteren kann hier bedeutsam sein, dass nicht nach der Sensibilität der erfassten Daten unterschieden wird. So können auch besonders schützenswerte Korrespondenz und Daten in das Netz der Geheimdienste fallen.

Somit ist der geheimdienstliche Zugriff auf das globale Telekommunikationsnetzwerk während der Datenübertragung aufgrund der gleichzeitigen Erfassung von Korrespondenzinhalten und -metadaten einschließlich sensibler Daten eine

[459] Siehe oben 1. Abschnitt, Unterabschnitt B. III. 2. a.–c.
[460] Siehe dazu bereits 1. Abschnitt B. III. 2. A. Vgl. außerdem *McAskill, Ewen u.a.*, „GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications" The Guardian, 21. Juni 2013, abrufbar unter http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [zuletzt abgerufen 02.12.2021].
[461] Siehe 1. Abschnitt B. III. 2. a.

grundsätzlich eingriffsintensive Form der geheimdienstlichen Informationsgewinnung.

(2) Beschaffung von Telekommunikationsdaten aus Servern von *Service Providern*

Die geheimdienstliche Beschaffung von Korrespondenzdaten aus Servern von *Service Providern* kann auf sehr unterschiedliche Art und Weise geschehen. Die Eingriffsintensität ist je nach konkreter Art der Beschaffung sehr variabel. So können *Service Provider* rigoros dazu verpflichtet werden, Inhalte der Korrespondenzen ihrer Kunden den Geheimdiensten zu übergeben. In der Regel erstreckt sich diese Form der Telekommunikationsüberwachung jedoch auf die alleinige Gewinnung von Metadaten der Korrespondenzen. Dass indes auch die Erfassung von Metadaten, insbesondere bei dauerhafter und systematischer Ausführung durchaus eine hohe Eingriffsintensität haben kann, wurde bereits oben ausgeführt.[462] Eine zusätzliche Analyse der Korrespondenzinhalte erhöht nichtsdestotrotz die gesamte Eingriffsintensität.

Das Beispiel des US-Überwachungsprogramms „*PRISM*“, das viele große Onlinedienstleister in diesen Überwachungsmechanismus involviert hat, zeigt deutlich, wie weitgehend diese Form der Überwachung reichen kann. Wenn nämlich globale Dienstleister wie *Facebook* oder *Google* geheimdienstliche Informationsquellen darstellen, kann kaum mehr daran gezweifelt werden, dass die virtuelle Persönlichkeitsphäre von Millionen Menschen in den Händen der Geheimdienste liegt.

Die Geheimdienste können die Anwendung dieser Methode der Überwachung auch hinsichtlich des betroffenen Personenkreises unproblematisch steuern. In einem konkreten Verdachtsfall können einerseits allein die Telekommunikationsdaten einer bestimmten verdächtigen Person eingefordert werden. Neben solch einer Einzelfallüberwachung können allerdings auch die Daten einer Vielzahl von Individuen beschafft werden. Somit ist auch hier eine Massenüberwachung möglich.

Sind *Service Provider* aufgrund von nationalen Vorschriften zur obligatorischen Vorratsdatenspeicherung dazu verpflichtet, die Korrespondenzdaten ihrer Nutzer zu speichern, kann die Dauer der Speicherungspflicht ein Faktor für die Eingriffsintensität sein.[463] Denn erfolgt die Datenspeicherung über einen langen Zeitraum, so werden über diese Zeitspanne hinweg auch quantitativ mehr Daten und Informationen über ein Individuum, das die Dienstleistung des *Service Providers* nutzt, gespeichert. Der Geheimdienst gewinnt dann beim Zugriff auf diesen Datensatz eines Individuums weitaus mehr Informationen als dies bei kürzeren Speicherfristen möglich wäre. Die Speicherfristen sind in den einzelnen Staaten unterschiedlich geregelt. Verständlicherweise besorgt hat sich der MRA hinsichtlich der in Kamerun für *Service Provider* gesetzlich vorgeschriebenen Speicherungsfrist von 10 Jahren

[462] Siehe 2. Abschnitt, Unterabschnitt II. 4. b. aa.

[463] Siehe dazu bereits 1. Abschnitt, Unterabschnitt B. III. 2. b.

gezeigt.[464] Hier gewinnt der Geheimdienst die Korrespondenz eines Jahrzehnts des betroffenen Individuums. Die Eingriffsintensität ist in solch einem Fall sehr hoch.

(3) Zugriff auf private Telekommunikationsgeräte

Die direkte Überwachung von privaten Telekommunikationsgeräten wird in aller Regel als Einzelfallmaßnahme und auf Grundlage eines konkreten Verdachts durchgeführt. Ein undifferenzierter geheimdienstlicher Zugriff auf eine hohe Anzahl von privatgenutzten Telekommunikationsgeräten ist aufgrund des technischen Aufwands nicht praktikabel.

Durch den Zugriff der Geheimdienste auf private Geräte, wie Computer oder Smartphones, werden nicht nur die Inhalte und Metadaten der mit den überwachten Geräten geführten Korrespondenz erfasst. Die Reichweite dieser Überwachungsform geht vielmehr weit darüber hinaus. Denn der Geheimdienst gewinnt mit dem direkten Zugriff auf persönliche Telekommunikationsgeräte Einsicht in den gesamten privaten Kommunikationskontext der Individuen. Jegliche Nachrichten, die von dem betroffenen Gerät verschickt oder empfangen sowie hierauf gespeichert sind, werden offengelegt. Die Geheimdienste erlangen nicht nur Kenntnis über die Inhalte der Nachrichten, sondern gewinnen auch ein umfassendes Bild über jegliche Adressaten und anderen Daten, die Aufschluss über die Korrespondenzgewohnheiten der Person geben. Sogar die Entstehungsphase einer Nachricht steht dabei unter Beobachtung. Üblicherweise können Individuen bis zum letzten Augenblick vor dem Absenden oder Äußern der Nachricht entscheiden, ob sie ihre Mitteilung tatsächlich aus der Hand geben möchten. Bei einer simultanen Überwachung während der Entstehungsphase, ist dieser persönliche Selektionsprozess praktisch aufgehoben. Bevor die Mitteilung überhaupt als Korrespondenz im Sinne der Art. 17 IPbpR sowie Art. 8 EMRK freigegeben wird, haben die Geheimdienste bei dieser Form der Ausspähung bereits Kenntnis über die Gedanken und den Willensbildungsprozess der Betroffenen gewonnen. Der Staat greift damit in einen äußerst sensiblen Bereich der Privatsphäre ein. Zudem ist nicht nur eine bestimmte Form der Korrespondenz Gegenstand der Überwachung. Vielmehr ist jegliche Korrespondenz, die über das betroffene Gerät abgewickelt wird, betroffen. Dabei sei an dieser Stelle darauf hingewiesen, dass die modernen Formen der digitalen, internetgestützten Telekommunikation weltweit von unzähligen Individuen intensiv genutzt werden.[465] Insofern kommt für diese Form der Überwachung nicht nur ein exklusiver Kreis einzelner Individuen in Betracht.

Zwar sind freilich nicht alle Daten, die auf den Geräten gespeichert sind und von den Geheimdienten eingesehen werden, Korrespondenzdaten im Sinne der Art. 17 IPbpR und Art. 8 EMRK. Jedoch können andere persönliche Daten, die auf den Geräten gespeichert sind und selbst keine Korrespondenz im Sinne der

[464] UN Human Rights Committee, Concluding observations: Cameroon, CCPR/C/CMR/CO/5, 30. November 2017, Rn. 39.

[465] Siehe 1. Abschnitt, Unterabschnitt A. II.

genannten Artikel darstellen, die in den Nachrichten und Korrespondenzen enthaltenen Informationen aufschlüsseln. Stehen diese Daten etwa in einem direkten Zusammenhang zu den Inhalten einzelner Korrespondenzen, so könnten die Geheimdienste durch eine ganzheitliche Analyse aller Daten weitaus mehr Informationen aus den Korrespondenzen gewinnen und nachvollziehen.

Somit wird deutlich, dass Geheimdienste mithilfe dieser Form der Telekommunikationsüberwachung ein sehr detailliertes Bild der betroffenen Personen gewinnen können. Der Eingriff in den Schutz der Privatsphäre kann in diesen Fällen in Abhängigkeit des konkreten Überwachungsumfangs damit sehr intensiv sein.[466]

bb. Zwischenergebnis

Die Ausführungen haben gezeigt, dass die Telekommunikationsüberwachung generell eine intensive geheimdienstliche Überwachungsform darstellt. Dabei kann der Intensitätsgrad einzelner Maßnahmen je nach Fallkonstellation variieren. Die konkrete Eingriffsintensität hängt von den Umständen des Einzelfalles ab. Dabei spielt einerseits die konkret angewendete Methodik zur Ausspähung der Korrespondenz eine wichtige Rolle. Aber auch Faktoren wie Dauer und Sensibilität der Daten können entscheidend die Intensität des Eingriffs beeinflussen. Insbesondere die Kumulation von mehreren Faktoren könnte im Einzelfall zu einer erheblichen Intensivierung des Eingriffs führen.

b. Schutzvorschriften und Rechtsmittel im nationalen Recht

In Fällen der Telekommunikationsüberwachung stellen sowohl der MRA als auch der EGMR für die Beurteilung der Verhältnismäßigkeit auf die nationalen Vorschriften und Sicherungsmechanismen zum Schutz vor Missbrauch von heimlichen Überwachungsmaßnahmen ab. Der EGMR stellt in einschlägigen Fällen regelmäßig Folgendes vorweg fest:

> „In view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective.“[467]

Gerade in der Geheimheit von Telekommunikationsüberwachungsmaßnahmen steckt eine erhöhte Gefahr für staatlichen Machtmissbrauch.[468] Die Qualität der

---

[466] Vgl. auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 38.

[467] EGMR, *Dragojević v. Croatia,* Rs. 68955/11, 15. Januar 2015, Rn. 83; siehe außerdem *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 57; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232.

[468] EGMR, *Malone v. The United Kingdom*, Rs. 8691/79, 26. April 1985, Serie A 95, Rn. 67: „Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident“.

Schutzvorschriften und der Rechtsbehelfe eines Überwachungsregimes entscheiden letztlich über die Verhältnismäßigkeit und Rechtmäßigkeit der Überwachungsmaßnahmen. Insofern kommt es für die Verhältnismäßigkeit der Überwachungsmaßnahmen – neben der Gewichtung des staatlichen Ziels und der Eingriffsintensität – auch auf die Schutzvorschriften in den einschlägigen nationalen Rechtnormen an. Konkret geht es dabei einerseits um die Frage, wie die Genehmigung und die Aufsicht von geheimen Überwachungsmaßnahmen reguliert sind. Des Weiteren ist das Vorhandensein effektiver Rechtsbehelfe für betroffene Individuen von entscheidender Bedeutung. Je intensiver und weitreichender Überwachungsmaßnahmen sind, umso höhere Anforderungen sind an die niedergelegten Schutzvorschriften und Rechtsbehelfen zu stellen.

aa. Unabhängige Genehmigung und Aufsicht der Überwachungsmaßnahmen

Die Überwachungsvorschriften müssen ein funktionierendes Schutzsystem schaffen, um eine missbräuchliche Anwendung von Überwachungsmaßnahmen durch den Staat bestmöglich zu verhindern. Dabei kommt es einerseits insbesondere darauf an, ob die nationalen Behörden, die für die Genehmigung und Aufsicht von Überwachungsmaßnahmen zuständig sind, unabhängig agieren. Außerdem muss im gesamten Prozess von Überwachungsmaßnahmen eine Zuständigkeitsaufteilung zwischen den Staatsgewalten erkennbar sein.[469]

Hinsichtlich des Genehmigungsverfahrens hebt der MRA in seinen *Concluding Observations* regelmäßig hervor, dass Telekommunikationsüberwachungsmaßnahmen eine richterliche Ermächtigung bedürfen.[470] Zumindest müsse die Judikative im Genehmigungsverfahren involviert sein.[471] Auch im Fall *Antonius Cornelis Van Hulst v. The Netherlands* hat der Ausschuss in seiner Argumentation festgestellt, dass in dem konkreten Fall die Überwachung des Beschwerdeführers von einem Richter

---

[469] Vgl. Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 37 sowie Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 40.

[470] UN Human Rights Committee, Concluding observations: Turkmenistan, CCPR/C/TKM/CO/2, 20. April 2017, Rn. 37; Concluding observations: South Africa, CCPR/C/ZAF/CO/1, 27. April 2016, Rn. 43; Concluding observations: Australia, CCPR/C/AUS/CO/6, 1. Dezember 2017, Rn. 45; Concluding observations: Belarus, CCPR/C/BLR/CO/5, 22. November 2018, Rn. 44; Concluding observations: Equatorial Guinea, CCPR/C/GNQ/CO/1, 22. August 2019, Rn. 51; Concluding observations: Finland, CCPR/C/FIN/CO/7, 3. Mai 2021, Rn. 35; Concluding observations: Tajikistan, CCPR/C/TJK/CO/3, 22. August 2019, Rn. 42.

[471] UN Human Rights Committee, Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37; Concluding observations: Rwanda, CCPR/C/RWA/CO/4, 2. Mai 2016, Rn. 35, 36; Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; Concluding observations: Canada, CCPR/C/CAN/CO/6, 13. August 2015, Rn. 10; Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12; Concluding observations: USA, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22.

schriftlich angeordnet wurde.[472] Bislang geht einzig aus den ergangenen *Concluding Observations* für Estland ausdrücklich hervor, dass auch andere unabhängige Organe eine Genehmigung von Überwachungsmaßnahmen vornehmen dürften.[473] Diesen Standpunkt vertritt der EGMR schon seit längerer Zeit. Nach Ansicht des EGMR kann die Genehmigung von Überwachungsmaßnahmen nämlich auch durch nicht-juristische Behörden mit der EMRK vereinbar sein, solange die zuständigen Behörden unabhängig von der Exekutive agieren.[474] Eine gerichtliche Genehmigung entfalte zwar durchaus eine wichtige Schutzwirkung vor Machtmissbrauch, jedoch sei dies nach Ansicht des EGMR keine zwingende Voraussetzung.[475] Die zuständige Behörde muss Zugang zu allen relevanten Materialen haben, um die Entscheidung über die Erteilung einer Genehmigung aufgrund einer substantiellen Begründungsbasis und unter Berücksichtigung aller Hintergrundfakten treffen zu können.[476] Der EGMR hat in diesem Zusammenhang außerdem klargestellt, dass die zuständigen unabhängigen Behörden für die Erteilung einer Genehmigung ausführlich begründen müssen, dass eine zwingende Notwendigkeit für die Anordnung geheimer Überwachungsmaßnahmen bestehe.[477]

Neben der unabhängigen Genehmigung ist zudem ein effektives und unabhängiges Aufsichtssystem eine besonders bedeutsame nationale Schutzmaßnahme. Jegliche geheimdienstliche Maßnahme zur Telekommunikationsüberwachung muss demnach durch spezielle unabhängige Gremien kontrolliert und beaufsichtigt werden. Rechtsverstöße durch die Überwachungsorgane können so etwa bereits frühzeitig identifiziert und damit gegebenenfalls resultierende Verletzungen von Menschenrechten potenziell betroffener Individuen verhindert werden.

Im Gegensatz zu seiner Rechtsprechung für das Genehmigungsverfahren, setzt der EGMR für das Aufsichtsverfahren einen strengeren Maßstab an und zieht grundsätzlich ein juristisches Organ zur Durchführung der Überwachungsaufsicht vor:

> „The Court recalls that the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at

---

[472] UN Human Rights Committee, *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004, Rn. 7.7.

[473] UN Human Rights Committee, Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 30.

[474] EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 258 m.w.N.

[475] EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 250.

[476] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 377 f.

[477] EGMR, *Dragojević v. Croatia,* Rs. 68955/11, 15. Januar 2015, Rn. 94; *Iordachi and Others v. Moldova,* Rs. 25198/02, 10. Februar 2009, Rn. 51.

> least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.“[478]

Somit ist nach Ansicht des EGMR eine richterliche Aufsicht von Überwachungsmaßnahmen wünschenswert. So können dieser Rechtsprechung zufolge sogar Defizite im Genehmigungsverfahren anschließend durch unabhängige richterliche Aufsichtsmechanismen ausgeglichen und korrigiert werden:

> „The Court recalls that […] either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body’s activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule […]. The ex ante authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation“.[479]

Dennoch zieht auch hier der Gerichtshof keine starren Grenzen. Im Einzelfall kann auch eine Aufsicht durch nicht-juristische Behörden mit der EMRK vereinbar sein. Die Voraussetzungen hierfür hat der EGMR etwa in der Entscheidung *Roman Zakharov v. Russia* benannt:

> „Although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control“.[480]

Dies hat der EGMR bereits in der Entscheidung *Klass and Others v. Germany* hinsichtlich des deutschen G-10-Gesetzes geäußert. So stellte der Gerichtshof in dieser Entscheidung fest, dass das deutsche G-10-Gesetz zwar keine juristische Aufsicht normiere, allerdings einen unabhängigen und effektiven Aufsichtsmechanismus reguliert, der mit den Voraussetzungen des Art. 8 EMRK vereinbar sei. So agierten das Parlamentarische Kontrollgremium sowie die G-10-Kommission als Aufsichtsorgane unter dem G-10 Gesetz unabhängig von den Überwachungsorganen. Zudem hebt der EGMR die ausgewogene Zusammensetzung des Parlamentarischen

---

[478] EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 77. Siehe auch EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 56; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 233, 275.

[479] EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 77.

[480] EGMR, *Roman Zakharov v. Russia [GC],* Rs. 47143/06, 4. Dezember 2015, Rn. 275.

Kontrollgremiums, in dem auch Oppositionsmitglieder beteiligt sind, hervor.[481] Auch sei der unter dem britischen Gesetz RIPA eigens als Aufsichtsorgan vom Premierminister ernannte Kommissar für Telekommunikationsüberwachung, der als Voraussetzung in seiner Person ein hohes juristisches Amt innehaben muss oder musste, in seiner Funktion als Aufsichtsorgan hinreichend unabhängig. Dies stellte der EGMR im Fall *Kennedy v. The United Kingdom* fest und bestätigte dies zudem im Fall *Big Brother Watch and Others v. The United Kingdom*.[482] In der Entscheidung *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* hat der EGMR hingegen die Unabhängigkeit des Innenministers, der nach bulgarischem Recht für die Aufsicht von geheimen Überwachungsmaßnahmen der Telekommunikation zuständig war, verneint. So sei der Innenminister einerseits ein Organ der Exekutive und darüber hinaus in der Anordnung von Überwachungsmaßnahmen direkt involviert.[483] Somit wird deutlich, dass der EGMR den Mitgliedstaaten einen weiten Spielraum in der Gestaltung des Genehmigungs- und Aufsichtsverfahrens von Überwachungsmaßnahmen überlässt. Zwar betont der Gerichtshof, dass gerade für das Aufsichtsverfahren die Einbeziehung eines Richters die Regel sein sollte, hält dies allerdings nicht für zwingend. Vielmehr kommt es auf die Unabhängigkeit der zuständigen Behörden an, um einen effektiven Schutz vor Missbrauch von Telekommunikationsüberwachungsmaßnahmen zu gewähren.

Der Menschenrechtsausschuss hat bislang in einzelnen *Concluding Observations* die entsprechenden Staaten dazu aufgefordert, die Judikative in die Aufsicht von Überwachungsmaßnahmen einzubeziehen.[484] Allerdings verlangt der Ausschuss in der überwiegenden Mehrheit der *Concluding Observations*, die unter anderem auch staatliche Überwachungsmaßnahmen betreffen, dass effektive und unabhängige Aufsichtsmechanismen über die Telekommunikationsüberwachung eingerichtet werden

---

[481] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 56. Siehe in diesem Zusammenhang auch EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 117. Außerdem EGMR, *Leander v. Sweden*, Rs. 9248/81, 26. März 1987, Series A116, Rn. 65; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 278. Zu den nachrichtendienstlichen Aufsichtsorganen in Deutschland (Parlamentarisches Kontrollgremium und die G-10-Komission) siehe *Friedel,* Blackbox. Parlamentarisches Kontrollgremium des Bundestags, S. 259 ff. Zum deutschen G-10 Gesetz siehe *Schaller*, Strategic Surveillance and Extraterritorial Basic Rights Protection, S. 948 ff.

[482] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 166; *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 135 f., 407.

[483] EGMR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Rs. 62540/00, 28. Juni 2007, Rn. 87. Im Fall *Iordachi and Others v. Moldova,* Rs. 25198/02, 10. Februar 2009, Rn. 47 verneinte der EGMR die Unabhängigkeit der Staatsanwaltschaft als zuständige Aufsichtsbehörde für Überwachungsmaßnahmen.

[484] Siehe etwa UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12; Concluding observations: Rwanda, CCPR/C/RWA/CO/4, 2. Mai 2016, Rn. 36; Concluding observations: Zimbabwe, CCPR/C/79/Add. 89, 6. April 1998, Rn. 25.

müssten, ohne dabei die Judikative ausdrücklich zu benennen.[485] So heißt es beispielsweise in den *Concluding Observations* für Canada:

> „The State party should [...] establish oversight mechanisms over security and intelligence agencies that are effective and adequate, and provide them with appropriate powers as well as sufficient resources to carry out their mandate".[486]

Demzufolge hält der Menschenrechtsausschuss für eine Vereinbarkeit von Überwachungsmaßnahmen mit Art. 17 IPbpR eine richterliche Aufsicht nicht für zwingend erforderlich. Die Aufsicht müsse allein effektiv und unabhängig erfolgen. Auch im OHCHR-Bericht zum Schutz der Privatsphäre im digitalen Zeitalter wird betont, dass eine nicht-juristische Aufsicht von Überwachungsmaßnahmen durchaus mit Art. 17 IPbpR vereinbar sein kann:

> „At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight […]."[487]

Der Bericht stellt insofern ausdrücklich heraus, dass juristische Aufsichtsverfahren in einzelnen Ländern sogar rein formale Verfahren sind, ohne dass dabei substanzielle Überprüfungen stattfinden. Insofern garantiert eine juristische Aufsichtsdurchführung keineswegs immer die Effektivität des Verfahrens. Die Einbeziehung mehrerer Gewalten in die Aufsicht von Überwachungsmaßnahmen würde dem OHCHR zufolge eher zu einer effektiven Durchführung der Aufsicht führen.

---

[485] UN Human Rights Committee, Concluding observations: Norway, CCPR/C/NOR/CO/7, 25. April 2018, Rn. 21; Concluding observations: Hungary, CCPR/C/HUN/CO/6, 9. Mai 2018, Rn. 44; Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37; Turkmenistan, CCPR/C/TKM/CO/2, 20. April 2017, Rn. 37; Concluding observations: Marocco, CCPR/C /MAR/CO/6, 1. Dezember 2016, Rn. 38; Concluding observations: Sweden, CCPR/C/SWE/ CO/7, 28. April 2016, Rn. 37; Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; Concluding observations: Canada, CCPR/C/CAN/CO/6, 13. August 2015, Rn. 10; Concluding observations: USA, CCPR/C/ USA/CO/4, 23. April 2014, Rn. 22; Concluding observations: Sweden, CCPR/C/SWE/CO/6, 7. Mai 2009, Rn. 18; Concluding observations, Poland, CCPR/C/79/Add. 110, 29. Juli 1999, Rn. 22; Concluding observations: Equatorial Guinea, CCPR/C/GNQ/CO/1, 22. August 2019, Rn. 51.

[486] UN Human Rights Committee, Concluding observations: Canada, CCPR/C/CAN/CO/6, 13. August 2015, Rn. 10.

[487] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 38.

bb. Effektive Rechtsbehelfe

Schließlich ist für den Schutz vor staatlichen Machtmissbrauch im Bereich der Telekommunikationsüberwachung ausschlaggebend, ob die einschlägigen nationalen Rechtsnormen betroffenen Individuen effektive Rechtsbehelfe zur Geltendmachung von Rechtsverletzungen durch Überwachungsmaßnahmen gewähren. Während im Rahmen der Genehmigungsanforderungen und der Aufsichtsverfahren eine staatliche Überprüfung der Überwachung stattfindet, schaffen Rechtsbehelfe eine Möglichkeit, dass sich betroffene Individuen selbst aktiv gegen Rechtsverletzungen zur Wehr setzen.

Sowohl der MRA als auch der EGMR haben in ihrer Spruchpraxis die Bedeutsamkeit von effektiven Rechtsbehelfen nachdrücklich hervorgehoben.[488] Entscheidend ist, dass die Rechtsbehelfe dabei nicht nur theoretisch bestehen, sondern in der Praxis effektive Wirkung entfalten. In diesem Sinne müssen die zur Verfügung stehenden Rechtsbehelfe in den Gesetzen ausdrücklich niedergelegt sein und zudem in der Praxis auch durchgesetzt werden.[489] Allein aus dieser Kombination kann eine effektive Wirkung der Rechtsbehelfe erzielt werden. Dabei spielen konkrete Faktoren für die praktische Effektivität eine essenzielle Rolle. Einerseits müssen die Rechtsbehelfe gegen geheimdienstliche Maßnahmen zur Telekommunikationsüberwachung den potenziell betroffenen Individuen selbstverständlich bekannt und zugänglich sein. Denn anderenfalls wäre eine Inanspruchnahme der Rechtsbehelfe praktisch ausgeschlossen.[490]

Aber nicht nur die Kenntnis über die Existenz der Rechtsbehelfe ist wichtig. Denn darüber hinaus ist die Kenntnis über die geheimdienstliche Durchführung von Überwachungsmaßnahmen eine entscheidende Grundvoraussetzung für die Effektivität von jeglichen Rechtsbehelfen im Bereich der Telekommunikationsüberwachung.[491] Das Individuum muss darüber Kenntnis haben, dass seine Telekommunikation überwacht wurde. Dies ist bei geheimen Überwachungsmaßnahmen in der Regel jedoch nicht der Fall. Wissen betroffene Individuen wiederum nicht von der Überwachungsdurchführung, so können sie auch keine Rechtsbehelfe einlegen, auch wenn ihnen dieses Recht gesetzlich eingeräumt wird. Insofern muss für eine praktische Effektivität der Rechtsbehelfe eine Benachrichtigung über die Maßnahmen erfolgen, damit Individuen überhaupt die Möglichkeit haben, sich

[488] Dies hat der MRA insbesondere in einer Reihe von *Concluding Observations* festgestellt, so etwa auch in UN Human Rights Committee, Concluding observations: Lebanon, CCPR/C/LBN/CO/3, 9. Mai 2018, Rn. 34; Concluding observations: Turkmenistan, CCPR/C/TKM/CO/2, 20. April 2017, Rn. 37. Siehe auch die ständige Rechtsprechung des EGMR, so etwa in *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 232.

[489] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 39.

[490] Vgl. Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 40.

[491] Siehe etwa EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 135.

dagegen zur Wehr zu setzen. Wie auch der EGMR in seiner Spruchpraxis festgestellt hat, können betroffene Individuen theoretisch vor, während oder nach der Durchführung von Überwachungsmaßnahmen informiert werden.[492] Dass allerdings die ersten beiden Alternativen mit dem Wesen und dem Zweck von geheimen Telekommunikationsüberwachungen nicht vereinbar sind, steht außer Frage. So spielt in der Praxis und so auch in der Jurisprudenz des MRA und des EGMR eine *ex post* Benachrichtigung von betroffenen Individuen eine Rolle. Der MRA hat sich erst in neueren *Concluding Observations* mit dem Thema der Benachrichtigung von Individuen, die durch nationale Überwachungsmaßnahmen betroffen waren, befasst.[493] In den *Concluding Observations* für den Staatenbericht Italiens hat der Ausschuss etwa ausdrücklich dazu aufgefordert, eine *ex post* Benachrichtigung von betroffenen Individuen einzuführen.[494] Die Spruchpraxis des EGMR ist auch in diesem Bereich umfangreicher. So hat sich der EGMR bereits im Fall *Klass and Others v. Germany* mit dem Thema der Benachrichtigung von überwachten Individuen befasst.[495] Der Gerichtshof spricht sich in seiner Jurisprudenz durchaus grundsätzlich für eine Verpflichtung zur nachträglichen Informierung von Individuen, die überwacht wurden, aus.[496] Allerdings lässt der Gerichtshof auch in diesem Bereich Ausnahmen zu. So stellte der Gerichtshof in einigen Urteilen zunächst fest, dass Benachrichtigungspflichten die Ziele der Überwachungsmaßnahmen gefährden können.[497] Dies gilt insbesondere in Fällen, in denen geheimdienstliche Überwachungsmaßnahmen aufgrund eines besonderen Sachverhaltes über einen langen Zeitraum geplant und durchgeführt werden. Eine sofortige Benachrichtigung der überwachten Individuen nach jeder einzelnen Etappe der langfristigen Überwachung würde freilich den Zweck solcher Überwachungsprogramme wesentlich gefährden.[498] Vor diesem Hintergrund führe nicht jedes Ausbleiben einer sofortigen Benachrichtigung

[492] Vgl. EGMR, *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 233.
[493] UN Human Rights Committee, Concluding observations, Poland, CCPR/C/POL/CO/7, 23. November 2016, Rn. 39; Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37; Concluding observations: Hungary, CCPR/C/HUN/CO/6, 9. Mai 2018, Rn. 43; Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 30; Concluding observations: Netherlands, CCPR/C/NLD/CO/5, 22. August 2019, Rn. 54.
[494] UN Human Rights Committee, Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37.
[495] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 57 ff.
[496] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 57 f.; *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 135; *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 86; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 234; *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 337.
[497] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 58; *Leander v. Sweden*, Rs. 9248/81, 26. März 1987, Series A116, Rn. 66; *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 135; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 287.
[498] EGMR, *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28, Rn. 58; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 287.

automatisch zur Unverhältnismäßigkeit der Maßnahme.[499] Sobald allerdings in solchen Fällen eine Benachrichtigung der Individuen möglich sei, ohne dass die Überwachungsziele gefährdet würden, sollte dies auch erfolgen. Des Weiteren seien auch nationale Überwachungsgesetze ohne obligatorische Benachrichtigungsvorschriften mit der EMRK vereinbar, wenn eine gerichtliche Überprüfung nicht von der Unterrichtung der Individuen abhängt. Können sich Individuen, die den Verdacht haben, dass ihre Telekommunikation Gegenstand geheimdienstlicher Überwachung geworden ist, an die für eine Überprüfung des Sachverhalts zuständigen Gerichte wenden, so sei nach Ansicht des EGMR eine verpflichtende nachträgliche Benachrichtigung nicht mehr zwingend notwendig.[500]

Ein weiterer Faktor für die Effektivität von Rechtsmitteln ist eine ausschöpfende und unverzügliche Ermittlung der Vorwürfe durch unabhängige staatliche Organe. So muss ein ordnungsgemäßes Ermittlungsverfahren im Gesetz vorgesehen sein und in der Praxis gewährleistet werden. Wendet sich ein Individuum mit der Behauptung an die zuständigen Gerichte, dass seine Telekommunikation durch geheimdienstliche Maßnahmen überwacht worden sei, muss im Rahmen eines Ermittlungsverfahrens der Sachverhalt aufgeklärt werden.[501]

Schließlich erfordert jeder effektive Rechtsbehelf, dass dem Individuum bei Begründetheit der Beschwerde abgeholfen wird und eine Beendigung der Rechtsverletzung vorgenommen wird. Im Kontext der Telekommunikationsüberwachung bedeutet dies in erster Linie, dass andauernde unrechtmäßige Überwachungsmaßnahmen beendet werden. Ist die Überwachung bereits abgeschlossen, müssen unrechtmäßig erlangte Daten etwa gelöscht und vernichtet werden, sofern keine zwingenden Gründe gegen eine Löschung sprechen.[502]

[499] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 135.

[500] EGMR, *Kennedy v. The United Kingdom*, Rs. 26839/05, 18. Mai 2010, Rn. 167; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 288. Dahingegen hat der EGMR im Fall *Szabó and Vissy* festgestellt, dass die ungarischen Gesetze aufgrund des Fehlens von Benachrichtigungsvorschriften keine ausreichenden Schutzmaßnahmen niederlegen. Dies begründet der Gerichtshof indes damit, dass zugleich keine effektiven formellen Rechtsbehelfe vorgesehen waren. Siehe EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 86.

[501] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 41.

[502] Ebd.

5. Undifferenzierte Massenüberwachung: Vereinbar mit Art. 17 IPbpR und Art. 8 EMRK?

Massenüberwachungssysteme sind in der heutigen Welt zu einem sicherheitspolitischen Bedürfnis der Staaten geworden und werden inzwischen in einigen Staaten praktiziert.[503] Diese moderne Form der Telekommunikationsüberwachung ist letztlich aufgrund der komplexen Gefährdungslage im nationalen und internationalen Raum entstanden. Geheimdienste erhoffen sich durch die Massenüberwachung auf Gefahrenindizien zu stoßen, um den künftigen Eintritt der Gefahren zu verhindern. Wie bereits im Kapitel der Funktion der geheimdienstlichen Spionage geschildert, stellen Dezentralisierung und Unvorhersehbarkeit des modernen internationalen Terrorismus besondere Herausforderungen für die staatlichen Sicherheitsbehörden dar.[504] Durch flächendeckende und undifferenzierte Formen der Überwachung können auch einzelne gefährliche Individuen eher ausfindig gemacht werden. Autonom agierende Individuen, die aus der Mitte der Bevölkerung agieren und terroristische Handlungen planen, können durch die massenhafte Überwachung aller Personen gefunden werden. Grundlage der Massenüberwachung ist mithin nicht ein konkreter Verdacht, sondern eine allgemeine Gefahrenlage. Somit ist die massenhafte Telekommunikationsüberwachung aus Sicht der Staaten durchaus ein geeignetes Mittel für die Sicherung der nationalen Sicherheit.

Damit verbunden ist jedoch die Frage, inwieweit solch ein weitreichendes Überwachungssystem den Anforderungen aus Art. 17 IPbpR und Art. 8 EMRK standhalten kann. Denn die oben aufgeführten Kriterien für die Rechtfertigung von Überwachungsmaßnahmen müssen grundsätzlich auch von geheimdienstlichen Maßnahmen zur Massenüberwachung erfüllt werden. Dabei wurde bereits aufgezeigt, dass Massenüberwachungsregime gerade keine Personendefinition vorsehen. Damit wäre streng genommen das Kriterium der Bestimmtheit der gesetzlichen Grundlage („*Foreseeability*“) gerade nicht erfüllt. Insofern ist fraglich, ob und inwieweit die vom MRA und EGMR anerkannten Kriterien zur Beurteilung der Menschenrechtskonformität von Überwachungsmaßnahmen auf den speziellen Fall der Massenüberwachung anzuwenden sind. Im Zuge ihrer Rechtsprechung haben sich bereits beide Spruchkörper mit dem Phänomen der Massenüberwachung befasst und allgemeine Feststellungen über die grundsätzliche Vereinbarkeit mit den Menschenrechtspakten getroffen. Nachfolgend wird diese Rechtsprechung jeweils aufgezeigt.

---

[503] Siehe hierzu den Bericht von *Amnesty International*, Dangerously disproportionate: The ever-expanding national security state in Europe (2017), abrufbar unter https://www.amnesty.org/en/documents/eur01/5342/2017/en/ [zuletzt abgerufen 02.12.2021].

[504] Siehe 1. Abschnitt, Unterabschnitt B. II.

a. Die Position des MRA

Da Massenüberwachungssysteme inzwischen in zahlreichen Staaten zum üblichen Programm ihrer geheimdienstlichen Telekommunikationsüberwachung zählen, ist diese Praxis auch regelmäßig Gegenstand der Staatenberichtsverfahren unter Art. 40 IPbpR.[505] Insofern hat sich der MRA im Rahmen der Staatenberichtsverfahren bislang häufig mit nationalen Massenüberwachungssystemen auseinandersetzen müssen. Dabei hat sich der MRA in den entsprechenden *Concluding Observations* unmissverständlich besorgt und kritisch gegenüber solchen weitläufigen Überwachungssystemen gezeigt. So hat der Ausschuss in den *Concluding Observations* für den Staatenbericht Großbritanniens Besorgnis darüber bekundet, dass das Überwachungsregime des Staates eine Massenausspähung zulässt:

> „The Committee is concerned that the State party's current legal regime governing the interception of communications and communication data allows for mass interception of communications [...]".[506]

Eine ähnliche Stellungnahme ist in den *Concluding Observations* hinsichtlich des US-Staatenberichts von 2014 vorzufinden.[507]

In anderen *Concluding Observations* zeigt sich der Ausschuss darüber besorgt, dass die nationalen Gesetze den Überwachungsorganen weite Überwachungsbefugnisse einräumen und dies wiederum in eine Massenüberwachung resultieren könne. So etwa die Feststellung des Ausschusses in den *Concluding Observations* zum Staatenbericht Kanadas:

> „However, the Committee is concerned about information according to which (a) Bill C-51's amendments to the Canadian Security Intelligence Act confer a broad mandate and powers on the Canadian Security Intelligence Service to act domestically and abroad, thus potentially resulting in mass surveillance and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards".[508]

---

[505] Zu den obligatorischen Staatenberichtsverfahren nach Art. 40 IPbpR siehe auch oben 2. Abschnitt, Unterabschnitt A. I. 2. a.

[506] UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24.

[507] UN Human Rights Committee, Concluding observations: United States of America, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22: „The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States, through the *bulk phone metadata surveillance programme* (Section 215 of the USA PATRIOT Act) [...]" [Hervorh. d. Verf.].

[508] Human Rights Committee, Concluding observations: Canada, CCPR/C/CAN/CO/6, 13. August 2015, Rn. 10.

In ähnlicher Weise hat sich der Ausschuss hinsichtlich weitläufiger Regularien in Dänemark ausgedrückt.[509] Die Äußerungen des Ausschusses deuten darauf hin, dass er diese spezielle Methode der Überwachung als eingriffsintensiv bewertet. Hierfür sprechen auch die *Concluding Observations* zum südafrikanischen Staatenbericht, in denen er ebenso seine kritische Haltung zur Massenüberwachung ausgedrückt hat:

> „The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre. [...] The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties".[510]

Aus dem ersten Satz der zitierten *Concluding Observations* könnte einerseits abgeleitet werden, dass Massenüberwachungen nach Ansicht des MRA grundsätzlich unrechtmäßig sind. Denn als Beispiel für die „*unlawful surveillance practices*" in Südafrika benennt der Ausschuss ausdrücklich die von den zuständigen nationalen Behörden ausgeführten Massenausspähungen. Entweder hält der MRA somit Massenausspähungen generell für unrechtmäßig. Die Aussage des Ausschusses könnte allerdings auch so ausgelegt werden, dass der Ausschuss die konkrete – möglicherweise mit den Anforderungen aus Art. 17 IPbpR unvereinbare – Art der Ausführung der Massenüberwachung durch das südafrikanische „*National Communications Centre*" für unrechtmäßig hält. Für diese Interpretation spricht auch der zweite Satz aus den zitierten *Concluding Observations*. Denn dieser Satz macht deutlich, dass der MRA eine Rechtfertigung von Massenüberwachungsmaßnahmen nicht ausschließt. Indem er nämlich betont, dass der Staat von einer Massenüberwachung ohne gerichtliche Genehmigung Abstand nehmen solle, bringt er die mögliche Vereinbarkeit mit Art. 17 IPbpR zum Ausdruck. Im Umkehrschluss bedeutet dies nämlich, dass bei Vorliegen einer gerichtlichen Autorisierung solcher Maßnahmen – und selbstverständlich auch aller anderen Voraussetzungen aus Art. 17 IPbpR – eine Rechtfertigung von Massenüberwachungsmaßnahmen möglich zu sein scheint.

Interessant ist auch die Aussage des MRA in den Concluding Observations, die zum Staatenbericht der Niederlande 2019 angenommen wurden.[511] Hier kritisiert

[509] UN Human Rights Committee, Concluding observations: Denmark, CCPR/C/DNK/CO/6, 15. August 2016, Rn. 28: „In particular, the Committee is concerned about: [...] b) section 780 of the Administration of Justice Act which allows interception of communication by the police domestically and which *may result in mass surveillance*, despite legal guarantees provided in section 781 and 783 of the same Act" [Hervorh. d. Verf.].

[510] UN Human Rights Committee, Concluding observations: South Africa, CCPR/C/ZAF/CO/1, 27. April 2016, Rn. 42–43.

[511] Human Rights Committee, Concluding observations: Netherlands, CCPR/C/NLD/CO/5, 22. August 2019, Rn. 54.

der Ausschuss nämlich das niederländische *Intelligence and Security Services Act 2017* u.a. in Hinblick darauf, dass eine „clear definition of case-specific bulk data collection“ nicht normiert sei.[512] Der Ausschuss bringt damit zum Ausdruck, dass eine Rechtfertigung von Massenüberwachungen auch von einer Definition der Umstände, die die Anordnung einer Massenüberwachung begründen, abhängt.

Die aufgezeigten *Concluding Observations* geben kein umfassendes Bild darüber, unter welchen Voraussetzungen nach Ansicht des MRA Massenüberwachungen mit Art. 17 IPbpR vereinbar sein können. Sie zeigen aber deutlich, dass nach Auffassung des MRA die Massenüberwachung eine eingriffsintensive Form der Telekommunikationsüberwachung ist. Die Aussagen des Ausschusses deuten zudem darauf hin, dass nach seiner Auffassung eine Rechtfertigung von Massenüberwachungsprogrammen nicht von vornherein ausgeschlossen ist. Die sehr kritische Haltung des Ausschusses und seine eindeutig zum Ausdruck gebrachte Besorgnis über nationale Massenüberwachungsprogramme belegen, dass wohl unter strenger Beachtung aller Voraussetzungen des Art. 17 IPbpR eine Rechtfertigung möglich ist.[513]

Auch die Interpretation des OHCHR in seinem Bericht zum Schutz der Privatsphäre im digitalen Zeitalter spricht für dieses Ergebnis.[514] Auf Grundlage der Aussagen des MRA im *General Comment* 27[515] stellt der OHCHR fest, dass die Staaten die Erforderlichkeit und Verhältnismäßigkeit von Massenüberwachungen beweisen müssten:

> „Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or ‚bulk‘ surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime.“[516]

---

[512] Ebd.

[513] Vgl. außerdem *Seibert-Fohr,* Digital Surveillance, Meta Data and Foreign Intelligence Cooperation, S. 11.

[514] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 25.

[515] UN Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), CCPR/C/21/Rev.1/Add. 9, 2. November 1999. Der OHCHR zitiert Auszüge aus den Rn. 11–16, in denen der Ausschuss Grundsätze hinsichtlich der Erforderlichkeit und Verhältnismäßigkeit von Eingriffen in Art. 12 IPbpR darstellt.

[516] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 25. Im letzten OHCHR-Bericht zum Recht der Privatsphäre im digitalen Zeitalter von 2018 wird noch deutlicher ausgesagt, dass Massenüberwachungen menschenrechtswidrig seien. Siehe Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 17.

Somit genügt nach Ansicht des OHCHR nicht, dass sich die Staaten allein auf den Zweck von Massenüberwachungen stützen.

b. Die Rechtsprechung des EGMR

aa. Die erste Phase der EGMR-Rechtsprechung

Der EGMR war in seiner Jurisprudenz in den vergangenen Jahren mit Fällen konfrontiert, in denen er über die Vereinbarkeit von Massenüberwachungsregimen mit Art. 8 EMRK entscheiden musste.[517]

Der Gerichtshof hat in der ersten Phase seiner einschlägigen Jurisprudenz festgestellt, dass auch Massenüberwachungsmaßnahmen im Rahmen des weiten Ermessensspielraums der Mitgliedstaaten grundsätzlich mit Art. 8 EMRK vereinbar sein können. So hat der Gerichtshof im Fall *Weber and Saravia v. Germany* die Vereinbarkeit des deutschen G-10-Gesetz, das unter anderem die Überwachung einer Vielzahl von Personen durch eine strategische Telekommunikationsausspähung mithilfe von Suchbegriffen regelte, mit Art. 8 EMRK geprüft.[518] Im Ergebnis wurde die Beschwerde als unzulässig abgewiesen. Dabei haben die Straßburger Richter insbesondere damit argumentiert, dass das geltende G-10-Gesetz ausreichende Mindestgarantien gegen willkürliche Eingriffe implementiere und zudem einen ausreichenden Schutz vor Machtmissbrauch gewähre.[519] In den Fällen *Liberty and Others v. The United Kingdom* und *Roman Zakharov v. Russia* hat der EGMR hingegen eine Verletzung von Art. 8 EMRK der Beschwerdeführer festgestellt.[520] In den jeweiligen Überwachungsgesetzen, die auch Massenausspähungen vorsahen, mangelte es nach Auffassung des Gerichtshofs unter anderem an effektiven Rechtsmitteln und hinreichenden Schutzvorschriften vor missbräuchlicher Anwendung durch die staatlichen Behörden. Dabei hat der EGMR in all diesen Fällen der ersten Phase keine strengeren Anforderungen an die Rechtfertigung von Massenüberwachungsregimen gestellt als für Einzelfallüberwachungen. Vielmehr hat der Gerichtshof in diesen Fällen der Massenüberwachung die in seiner Jurisprudenz entwickelten Mindestgarantien in gleicher Weise, wie er diese auch in Einzelüberwachungsfällen anwendet, durchgeprüft. So stellt der Gerichtshof im Fall *Liberty and Others v. The United Kingdom* etwa Folgendes fest:

---

[517] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI; EGMR, *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008.
[518] EGMR, *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI.
[519] Ebd., 137 f.
[520] EGMR, *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008, Rn. 69; *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015, Rn. 303 f.

> „The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."[521]

In dem 2016 entschiedenen Fall *Szabó and Vissy v. Hungary* deutet der EGMR indes erstmals einen strengeren Ansatz für Massenüberwachungen an. Gegenstand dieser Entscheidung war eine Vorschrift im ungarischen Polizeigesetz, das eine verdachtsunabhängige Überwachung von „Terrorverdächtigen" vorsah.[522] Auch hier hat der EGMR die entwickelten Mindestgarantien durchgeprüft. Allerdings hat der Gerichtshof hier erstmals die Auffassung vertreten, dass für Massenüberwachungsmaßnahmen strengere Maßstäbe im Rahmen der Verhältnismäßigkeit gelten müssten:

> „However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement ‚necessary in a democratic society' must be interpreted in this context as requiring ‚strict necessity' in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal."[523]

Damit schien der EGMR mit dieser Entscheidung in Orientierung an die – vom EGMR selbst ausdrücklich benannte[524] – Rechtsprechung des EuGH[525] einen neuen Weg für die Beurteilung von Massenüberwachungsmaßnahmen eingeschlagen zu haben. So könnte auf Grundlage dieses Urteils die Schlussfolgerung gezogen werden, dass der EGMR in Abweichung seiner zuvor ergangenen Urteile einen

[521] EGMR, *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008, Rn. 63.

[522] EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 8 ff.

[523] Ebd., Rn. 73.

[524] So heißt es in der Folge des oben zitierten Auszugs des *Szabó and Vissy* Urteils: „The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse." EGMR, *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016, Rn. 73.

[525] So hat der EuGH etwa im Fall *Digital Rights Ireland Ltd* festgestellt, dass Einschränkungen des Rechts auf Schutz personenbezogener Daten durch Massenüberwachungsmaßnahmen nur so weit gehen dürften, wie es unbedingt erforderlich sei. Siehe EuGH, *Digital Rights Ireland Ltd v. Minister for Communications & Others*, Rs. C-293/12 und C-594/12, 8. April 2014, Rn. 52.

Unterschied zwischen Einzelfallüberwachungen und Massenüberwachungen sieht.[526] Auch wenn der EGMR in dieser Entscheidung keine neuen Kriterien für den speziellen Fall der Massenüberwachung anwendet, so spricht er hier dennoch von einer „*strict necessity*". Der Gerichtshof legt hier einen strengen Maßstab an, wonach die staatliche Überwachungsmaßnahme einerseits zum Schutz der demokratischen Institutionen unbedingt notwendig sein und zudem auch der Gewinnung essenzieller Informationen im Rahmen einer „individuellen Operation" dienen müsse. Gerade das zweite Kriterium lässt die Folgerung zu, dass nur Einzelfallüberwachungen diesen strengen Maßstab erfüllen können.[527] Denn undifferenzierte Massenüberwachungen können kaum als „*individual operations*" gelten. Mit dem Urteil *Szabó and Vissy v. Hungary* deutet der EGMR an, dass für die Beurteilung der Verhältnismäßigkeit von Massenüberwachungen ein besonderes Maß anzuwenden sei.[528]

bb. Die Urteile Big Brother Watch and Others v. UK und Centrum för rättvisa v. Sweden

Eine neue Richtung in seiner Jurisprudenz schlägt der EGMR wenige Jahre später in den beiden Entscheidungen *Big Brother Watch and Others v. The United Kingdom*[529] und *Centrum för rättvisa v. Sweden*[530] ein.

Das Urteil *Big Brother Watch and Others v. The United Kingdom* basiert auf Beschwerden von Journalisten und Menschenrechtsorganisationen, die nach den NSA-Enthüllungen durch *Edward Snowden* eingereicht wurden.[531] Der Gerichtshof untersucht u.a. die Massenüberwachungen nach Abschnitt 8(4) des britischen RIPA.[532] Im zeitgleich ergangenen Urteil *Centrum för rättvisa v. Sweden*, das auf einer Beschwerde einer

---

526 Ähnlich argumentieren auch *Bignami/Resta*, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti/Nolte (Hrsg.), Community Interests Across International Law, S. 377 f.

527 So auch *St. Vincent,* Preventing the Police State, in Cate/Dempsey (Hrsg.), Bulk Collection, S. 373; *Psychogiopoulou*, The European Court of Human Rights, privacy and data protection in the digital era, in Brkan/Psychogiopoulou (Hrsg.), Courts, Privacy and Data Protection in the Digital Environment, S. 56.

528 *Bignami/Resta*, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti/Nolte (Hrsg.), Community Interests Across International Law, S. 377 f.

529 EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021.

530 EGMR*, Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021.

531 Bei den Beschwerdeführern handelt es sich um Datenschutz-NGOs wie Big Brother Watch, PEN und Open Rights Group sowie die deutsche Datenschutz-Expertin Constanze Kurz. Für die vollständige Auflistung der Beschwerdeführer siehe EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Appendix.

532 Das RIPA 2000 wurde inzwischen durch den *Investigatory Powers Act* 2016 ersetzt. Die Feststellungen der Großen Kammer beziehen sich jedoch ausschließlich auf die Bestimmungen des Gesetzes aus dem Jahr 2000, da dieses zum Zeitpunkt der Beschwerden die geltende Rechtsgrundlage darstellte. Vgl. EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 61. Zum Sachverhalts dieser Entscheidung siehe 1. Abschnitt B.III.2.a. sowie 2. Abschnitt B.I.1.b.

NGO in Stockholm basiert, prüft der EGMR die vom schwedischen Geheimdienst durchgeführte Massenüberwachung der Telekommunikation.[533]

In beiden Urteilen stellt der EGMR explizit fest, dass sich Massenüberwachungen von Einzelfallüberwachungen durchaus unterscheiden.[534] Somit müsse der für gezielte Einzelüberwachungen entwickelte Ansatz für die Fälle der Massenüberwachung angepasst werden.[535] Danach seien eine Bestimmung der betroffenen Personen sowie der konkreten überwachungsbegründenden Handlungen im Rahmen von Massenüberwachungen hinfällig. Denn die Massenüberwachung basiert gerade darauf, dass diese ohne konkreten Anlass verdachtsunabhängig durchgeführt wird und dabei gerade keine Personenbegrenzung im Voraus erfolgt. Stattdessen müssten die Überwachungsgesetze aber die Gründe für die Genehmigung der Überwachung sowie die Umstände, unter denen die Kommunikation einer Person abgehört werden kann, festlegen.[536] Dabei stellt der EGMR keine hohen Anforderungen an diese Kriterien. In der Entscheidung *Big Brother Watch and Others v. The United Kingdom* stellt der Gerichtshof beispielsweise fest, dass nach Abschnitt 5 (3) des RIPA die Genehmigung einer Massenüberwachung im Interesse der nationalen Sicherheit, zur Verhütung oder Aufdeckung schwerer Straftaten oder zur Wahrung des wirtschaftlichen Wohls des Vereinigten Königreichs möglich war.[537] Eine konkretere Definition der Überwachungsgründe war in diesem Gesetz nicht enthalten. Regelungen, die die Anordnung einer Massenüberwachung auf relativ breiter Basis erlaubten, sind nach Ansicht des EGMR mit Art. 8 EMRK vereinbar, sofern das System insgesamt ausreichende Garantien gegen Missbrauch biete.[538] Der EGMR befasst sich auch mit der in Massenüberwachungsregimen häufig vorzufindenden Begrenzung auf externe Telekommunikation. Nach diesen Regelungen sind von der Massenüberwachung theoretisch alle Telekommunikationsparteien ausgeschlossen, die innerhalb des Staates miteinander kommunizieren. Hierzu weist der EGMR indes darauf hin, dass die moderne Telekommunikationsinfrastruktur die Korrespondenzdaten nicht über den kürzesten Weg übermittelt, sodass auch inländische Telekommunikation über Leitungen im Ausland schließlich den inländischen Adressaten erreichen.[539] Der Geheimdienst erfasst in solchen Fällen somit auch diese scheinbar ausländische Korrespondenz, obwohl beide inländische Parteien eigentlich auf

[533] EGMR*, Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 10 ff.

[534] So zielten nach Auffassung des EGMR Massenüberwachungen insbesondere auf internationale Telekommunikation ab und diene der präventiven Aufdeckung sowie Bekämpfung von Cyberangriffen, der Spionageabwehr und der Bekämpfung von Terrorismus. Insbesondere aber sei die Missbrauchsgefahr im Rahmen der Massenüberwachung besonders erhöht, auf der anderen Seite aber auch das Bedürfnis der Staaten auf Geheimhaltung zu sehen. Vgl. EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 343 ff.

[535] Ebd., Rn. 347.

[536] EGMR*, Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 262.

[537] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 368.

[538] Ebd., Rn. 370.

[539] Ebd., Rn. 336. Siehe dazu bereits 1. Abschnitt, Unterabschnitt B. III. 2. a.

Grundlage des Gesetzes von der Überwachung ausgeschlossen sein sollten. Solch eine gesetzliche Begrenzung kann damit faktisch leerlaufen. Ein wichtiges Indiz zur Beurteilung solcher gesetzlichen Begrenzungen des Anwendungsbereiches der Überwachung kann nach Auffassung des EGMR darin bestehen, ob das Überwachungsgesetz und die Überwachungspraxis etwa im Rahmen von Direktzugriffen auf das Telekommunikationsnetzwerk auf solche Internetknotenpunkte konzentriert ist, die mit hoher Wahrscheinlichkeit relevante externe Nachrichten übermitteln.[540]

Die übrigen Kriterien, die für die Bestimmtheit von Überwachungsgesetzen maßgeblich sind, gelten indes auch für Massenüberwachungen. So müsse auch im Rahmen der Massenüberwachung gesetzlich die Dauer der Überwachung sowie das Verfahren zur Verarbeitung, die Weitergabe sowie die Löschung der erlangten Daten definiert werden.[541] Des Weiteren hebt der Gerichtshof hervor, dass insbesondere die Verhältnismäßigkeit der Maßnahme, ihre unabhängige Genehmigung und Beaufsichtigung sowie das Vorhandensein effektiver Rechtsbehelfe entscheidende Kriterien sind:

> „the Court considers that the process must be subject to ‚end-to-end safeguards', meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review."[542]

Ein sehr wichtiges Instrument der Geheimdienste zur Auswertung von Daten, die durch Massenüberwachungsmaßnahmen gewonnen werden, ist der anschließende Selektionsprozess. Erst durch die Anwendung von relevanten Suchbegriffen wird das gewonnene Datenmaterial gefiltert. Nur Daten, die von diesen Selektoren erfasst werden, gelangen in den weiteren Überwachungsapparat der Geheimdienste.[543] Der EGMR befasst sich in den Urteilen mit der Frage, inwieweit die Definierung der Selektoren im Voraus Gegenstand des Genehmigungsprozesses der Maßnahme sein muss. Wegen der wichtigen Bedeutung der Selektoren im Rahmen der Massenüberwachungen müsse die Genehmigung zumindest die Art oder die

---

[540] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 376.

[541] Ebd., Rn. 348; EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, 262.

[542] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 350.

[543] Die Anwendung von Selektoren ist in der Überwachungspraxis der Staaten etabliert. So sieht beispielsweise § 5 Abs. 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10 Gesetz) in Deutschland die Anwendung von Suchbegriffen im Rahmen von Strategischen Überwachungen vor.

Kategorien der Selektoren festlegen.[544] Strengere Anforderungen gelten nach Auffassung des Gerichtshofs nur bei Anwendung von sog. starken Selektoren.[545] Darunter sind solche Suchbegriffe zu verstehen, die konkret mit einem identifizierbaren Individuum zusammenhängen wie beispielsweise eine konkrete Emailadresse. Der Einsatz solcher Selektoren müsse im Voraus einem Verfahren der internen Genehmigung unterliegen, das eine gesonderte und objektive Überprüfung der Verhältnismäßigkeit und Rechtfertigung vorsieht.[546] Im Fall *Big Brother Watch and Others v. The United Kingdom* stellt der EGMR fest, dass der nach Abschnitt 8(4) RIPA für die Genehmigung zuständige *Secretary of State* kein von der Exekutive unabhängiges Organ sei sowie zudem die Selektoren und sogar die starken Selektoren nicht Gegenstand des Genehmigungsprozesses gewesen seien.[547] Im Gegensatz dazu sehe das schwedische System eine umfassende gerichtliche Überprüfung von Genehmigungsanträgen vor, das eine Kontrolle des Überwachungsziels, der betroffenen Internetknotenpunkte sowie die für Massenüberwachungen hinreichend definierten Kategorien der einzusetzenden Selektoren umfasse.[548]

Freilich prüft der EGMR auch im Rahmen dieser Urteile zur Massenüberwachung gründlich das Vorhandensein einer unabhängigen Aufsicht[549] und effektiver Rechtsbehelfe. Hinsichtlich der Rechtsbehelfe befasst sich der EGMR auch mit der Frage der Verpflichtung zur nachträglichen Information von betroffenen Individuen. Dabei stellt er in diesen Urteilen nunmehr deutlich fest, dass im Rahmen der Massenüberwachung eine nachträgliche Benachrichtigung von Individuen unpraktikabel sei:

> „The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location."[550]

---

[544] Ebd., Rn. 354; EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 268.

[545] Der EGMR spricht von „*strong selectors*", vgl. EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 269.

[546] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 355.

[547] Ebd., Rn. 377 ff., 383.

[548] EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 302.

[549] Hinsichtlich der Unabhängigkeit des für die Beaufsichtigung zuständigen Kommissars für Telekommunikationsüberwachung nach dem RIPA siehe bereits oben 2. Abschnitt B.II.4.b.aa.

[550] EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 272.

In Bekräftigung des Urteils *Roman Zakharov v. Russia* und anderer vorangegangener Urteile zu dieser Thematik stellt der EGMR fest, dass ein Rechtsbehelf auch dann effektiv sein könne, wenn Individuen allein mit dem Verdacht der Überwachung die Möglichkeit einer unabhängigen Überprüfung des Sachverhalts haben.[551] Das Vorhandensein solch eines soliden Rechtsbehelfs stellte der EGMR positiv im Fall *Big Brother Watch and Others v. The United Kingdom* fest. Das *Investigatory Powers Tribunal* sei eine gerichtliche Instanz, die unter den Vorschriften des RIPA eingerichtet wurde, um Beschwerden von Bürgern über unrechtmäßige Abhörung zu prüfen.[552] Die Überprüfung finde unabhängig von einer vorausgehenden Benachrichtigung über konkrete Überwachungsmaßnahmen statt.[553]

Schließlich befasst sich der EGMR in den Urteilen mit der Frage, ob die entwickelten Kriterien für Inhaltsdaten und Verbindungsdaten, die durch Massenüberwachung erlangt werden, gleichermaßen gelten. Hierzu stellt der Gerichtshof fest, dass die Erlangung von Metadaten nicht weniger intensiv sei.[554] Insofern gelten für die Abhörung von Inhalts- und Metadaten grundsätzlich der gleichen Anforderungen. Zugleich erkennt der Gerichtshof an, dass sich die Verbindungsdaten wesensmäßig von den Inhaltsdaten unterscheiden und von den Geheimdiensten anders verarbeitet und analysiert werden. Solange die geltenden Kriterien erfüllt werden, sei eine in jeder Hinsicht identische Behandlung der erlangten Inhalts- und Verbindungsdaten nicht zwingend.[555]

c. Würdigung und Ergebnis

Die Darstellung der Rechtsprechung zur Massenüberwachung hat offengelegt, dass die beiden Spruchkörper das Gefährdungspotenzial dieser Form des staatlichen Handelns für den Menschenrechtsschutz durchaus sehen. Der MRA hat eine grundsätzlich kritische Haltung eingenommen, die wohl tendenziell eine Rechtfertigung von Massenüberwachungsprogrammen nur unter strenger Berücksichtigung aller Kriterien des Art. 17 IPbpR zuzulassen scheint.[556] Der EGMR hat in der ersten Phase seiner Spruchpraxis die Massenüberwachung nach den gleichen Maßstäben, die für die Einzelfallüberwachung entwickelt wurden, beurteilt. In den Entscheidungen aus dem Jahr 2021 stellt er nunmehr einen modifizierten Kriterienkatalog auf. Dieser beurteilt Massenüberwachungen nicht strenger, allerdings sind die Kriterien an den spezifischen Eigenschaften der Massenüberwachung angepasst.

Tatsächlich muss für die Beurteilung der Verhältnismäßigkeit von Massenüberwachungen die besonderen Eigenschaften dieser weitreichenden Überwachungsform berücksichtigt werden. Hierbei geht es auch um Auswirkungen auf die

---

[551] Siehe dazu bereits 2. Abschnitt B.II.4.b.bb.
[552] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 413 ff.
[553] Ebd.
[554] Ebd., Rn. 363.
[555] Ebd., Rn. 364.
[556] Siehe dazu den vorangegangenen Unterabschnitt B. II. 4. d. aa.

gesamte Gesellschaft. Für den Einzelnen kann die Eingriffsintensität einer Massenüberwachung, die nicht gezielt Informationen eines konkreten Individuums herausfiltert, weniger intensiv sein als eine gezielte Einzelüberwachung. Gezielte und systematische Einzelfallüberwachung, etwa die Beobachtung von konkreten privatgenutzten Telekommunikationsgeräten über einen längeren Zeitraum, kann eine äußerst eingriffsintensive Spionageform sein. Solche einschneidenden Formen der gezielten Einzelfallüberwachung richten sich in der Regel gegen konkrete Individuen, die zumindest im dringenden Verdacht stehen, schwerwiegende Gefahren für die Allgemeinheit zu verursachen. In solch einer Fallkonstellation kann die sehr intensive geheimdienstliche Einzelfallüberwachung angesichts der konkreten Umstände und des erheblichen Gefahrenpotentials, die von den überwachten Individuen ausgeht, durchaus aufgrund der konkreten Interessenabwägung verhältnismäßig im Sinne der Art. 17 IPbpR sowie Art. 8 EMRK sein. Bei einer undifferenzierten Massenüberwachung kann die Eingriffsintensität hingegen gerade nicht mit den konkreten Eigenschaften all der betroffenen Personen ausgeglichen werden. Zwar mag die allgemeine Sicherheitslage im Staat brisant sein und sogar konkrete Terrorbedrohungen im staatspolitischen Raum stehen. Jedoch geht diese Gefahr nicht von all den beobachteten Personen aus. Auch wenn einzelne Individuen innerhalb der überwachten Masse als Gefährder enttarnt werden, steht dennoch der überragende Großteil dieser Individuen nicht einmal im geringsten Verdacht, eine Gefährdung für die staatliche Sicherheit zu verursachen. In solchen Fällen werden Millionen Personen beobachtet, um einzelne Individuen, die tatsächlich Gefahrenquellen sind, zu finden. Es geht hierbei also sprichwörtlich um die Suche nach der Nadel im Heuhaufen.[557] Wird im Rahmen der Massenüberwachung aufgrund von Suchfiltern die Beobachtung auf ein Individuum konzentriert, kann dies die Eingriffsintensität für dieses Individuum durchaus steigern. Allerdings könnte dies wiederum mit den Gefahren, die von diesem Individuum ausgehen, auch in Ausgleich gebracht werden.

Ein weiterer gesellschaftlicher Faktor ist das entstehende Klima des Beobachtet-Werdens innerhalb der Bevölkerung. Durch programmatische Massenüberwachungen entstehen in der breiten Bevölkerung ernsthafte Zweifel daran, ob die Vertraulichkeit ihrer Korrespondenzen gewahrt wird. Die Folge ist eine Form der Selbstzensur.[558] Werden nämlich alle Telekommunikationswege massenhaft überwacht, bleibt für betroffene Individuen als einziger Ausweg aus der Korrespondenz-

[557] Das Sprichwort der „Suche nach der Nadel im Heuhaufen“ wird in der Literatur häufig im Zusammenhang der Massenüberwachung verwendet. Siehe etwa den Aufsatz von *Taylor,* To find the needle do you need the whole haystack? Global surveillance and principled regulation.

[558] Vgl. auch European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democracy Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies (CDL-AD(2015)006), Venice, March 2015, Rn. 62. Siehe außerdem *Hermstrüwer,* Informationelle Selbstgefährdung, S. 41 ff; *PoKempner*, Cyberspace and State Obligations in the Area of Human Rights, in Zielkowski (Hrsg.), Peacetime regime for state activities in cyberspace, S. 252.

überwachung theoretisch nur der Verzicht auf moderne Formen der Telekommunikation.[559] Dies wäre angesichts der heutigen Etablierung dieser Telekommunikationstechnologie im alltäglichen Leben ein erheblicher Einschnitt in der individuellen Lebensgestaltung. Somit darf die Intensität von Massenüberwachungen im gesamtgesellschaftlichen Kontext keineswegs unterschätzt werden. Angesichts dieses Phänomens ist dem MRA und dem EGMR hinsichtlich des Vorhandenseins effektiver Rechtsbehelfe durchaus zuzustimmen. Effektive Rechtsbehelfe müssen gesetzlich geregelt sein und in der Praxis zur Verfügung stehen. Als wesentlicher Bestandteil der Effektivität der Rechtmittel muss auch im Fall der Massenüberwachung grundsätzlich ein System der nachfolgenden Benachrichtigung betroffener Individuen existieren.[560] Dem EGMR ist zwar zuzustimmen, dass im Rahmen von Massenüberwachungen solche Benachrichtigungen schwer umzusetzen sind.[561] Dies darf jedoch nicht zur Konsequenz haben, dass auf eine Benachrichtigung gänzlich verzichtet wird. Tatsächlich ist die Benachrichtigung von Millionen Menschen nicht nur hinsichtlich der Überwachungsziels fragwürdig, sondern auch in der Praxis tatsächlich kaum zu verwirklichen. Allerdings kann zumindest für die Personen, die aufgrund der Anwendung von bestimmten Suchkriterien in die engere Auswahl der Geheimdienste kommen, eine Benachrichtigung erfolgen. Darüber hinaus ist nach der Sichtweise des EGMR das Vorhandensein einer effektiven Verdachtsbeschwerde entscheidend. Die Möglichkeit, allein bei dem Verdacht der Überwachung eine Beschwerde einzureichen, die unabhängig und ernsthaft begutachtet wird, kann dem in der Gesellschaft entstehenden Klima, der Überwachung ausgeliefert zu sein, und der Selbstzensur entgegenwirken.

6. Ergebnis

Geheimdienstliche Telekommunikationsüberwachung kann mit dem Menschenrecht auf Privatsphäre gemäß Art. 17 IPbpR und Art. 8 EMRK vereinbar sein. Die Schrankenregelungen dieser Menschenrechte setzen klare und strikte Vorgaben über die Voraussetzungen, die erfüllt sein müssen, damit Maßnahmen zur Überwachung moderner Formen der individuellen Korrespondenz menschenrechtskonform sind. So müssen einerseits die nationalen Gesetzesgrundlagen die strengen Anforderungen der Zugänglichkeit und Bestimmtheit erfüllen. Zum Zwecke des Schutzes vor staatlichem Machtmissbrauch müssen die Individuen die Eingriffsbefugnisse des Staates, die sich aus der Anwendung der Gesetze ergeben, zumindest im Allgemeinen vorhersehen können. Im Rahmen des Erfordernisses der Verhältnismäßigkeit gelten weiterhin eine Reihe von besonderen Kriterien, die für die Überprüfung der Menschenrechtskonformität von Überwachungsmaßnahmen von großer Bedeutung sind. Hierbei spielen indes nicht nur die Gewichtung des staatlichen Zwecks der Überwachung und die Intensität des Eingriffs eine wichtige Rolle.

---

[559] Siehe dazu bereits oben 2. Abschnitt, unterabschnitt B I. 3. c.

[560] Siehe dazu 2. Abschnitt, Unterabschnitt B. II. 4. c. bb.

[561] Vgl. EGMR, *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021, Rn. 272.

Insbesondere ist darüber hinaus für die Verhältnismäßigkeit im Einzelfall entscheidend, ob unabhängige Aufsichtsmechanismen und effektive Rechtsbehelfe vorgesehen sind. Auf Grundlage dieser spezifischen Kriterien können nicht nur Einzelüberwachungen gerechtfertigt sein. Vielmehr ist auch die Vereinbarkeit von Massenüberwachungen mit Art. 17 IPbpR und Art. 8 EMRK nicht ausgeschlossen. Der in Art. 17 IPbpR und Art. 8 EMRK international verankerte Schutz der Vertraulichkeit der Korrespondenz und der personenbezogenen Daten erfasst damit auch modernste Formen der geheimdienstlichen Überwachung.

3. Abschnitt: Geheimdienstliche Telekommunikationsüberwachung außerhalb des Staatsgebiets

Geheimdienstliche Überwachungsmaßnahmen werden nicht nur innerhalb des eigenen Staatsgebiets ausgeführt. Vielmehr setzen die Staaten ihre geheimdienstlichen Mittel auch dafür ein, grenzüberschreitend Informationen zu gewinnen. Auch die moderne Telekommunikationsüberwachung endet nicht an den Staatsgrenzen. Die *Snowden*-Enthüllungen haben in dieser Hinsicht nur das Ausmaß dessen gezeigt, was schon seit Jahren übliche Praxis vieler Geheimdienste ist.

Im Rahmen extraterritorialer Überwachungsmaßnahmen drängt sich die Frage auf, ob und wie die involvierten Staaten ihre Menschenrechtsverpflichtungen aus den Pakten verletzen. Dabei wird im Folgenden der Staat, der die Überwachungsausübung außerhalb seines Territoriums anwendet, um die Telekommunikation von Individuen innerhalb eines anderen Staates auszuspähen, „Drittstaat" genannt. Der Staat, in dem sich das überwachte Individuum befindet, wird „Aufenthaltsstaat" genannt.

A. Verletzung des Schutzes der Privatsphäre durch Überwachungsmaßnahmen des Drittstaates

Im folgenden Unterabschnitt wird untersucht, inwieweit der Drittstaat aufgrund seiner grenzüberschreitenden Telekommunikationsüberwachung seine Menschenrechtsverpflichtungen aus Art. 17 IPbpR und Art. 8 EMRK verletzt. Da die Maßnahmen nicht innerhalb des eigenen Territoriums erfolgen, steht dabei die Frage nach der extraterritorialen Verpflichtung des Drittstaates unter den Menschenrechtspakten im Fokus.

I. Die extraterritoriale Anwendbarkeit des IPbpR und der EMRK: Allgemeine Grundlagen, Voraussetzungen und Rechtsfolgen

Nachfolgend wird anhand der einschlägigen Judikatur des MRA und des EGMR untersucht, ob die Menschenrechtspakte extraterritorial anwendbar sind und wodurch die extraterritoriale Anwendbarkeit ausgelöst wird. Anschließend wird dargestellt, wie die Reichweite der extraterritorialen Verpflichtungen der Staaten auf Rechtsfolgenseite ist.

1. Der territoriale Anwendungsbereich des IPbpR und der EMRK: Die Jurisdiktionsklauseln der beiden Menschenrechtspakte

„Jurisdiktion" ist ein weiter Begriff, der in vielen Bereichen des Staats- und Völkerrechts Verwendung findet und dabei jeweils unterschiedliche Bedeutungen hat.[562] In internationalen Menschenrechtsverträgen dienen Jurisdiktionsklauseln der Definition und Begrenzung des Anwendungsbereichs der Pakte.[563] „Jurisdiktion" im Sinne dieser Klauseln beschreibt dabei im weitesten Sinne die zwischen einem Staat und einem Individuum bestehende Beziehung, die durch die Gewalt des Staates über konkrete Personen oder über bestimmte Territorien, auf denen sich diese Personen befinden, begründet wird.[564] Aufgrund dieser Beziehung kann der betroffene Staat – je nach Formulierung der Jurisdiktionsklausel in einzelnen Menschenrechtsverträgen und der Auslegung durch die zuständigen Spruchkörper – gegenüber den unter seiner Gewalt stehenden Individuen zur Umsetzung der Paktbestimmungen verpflichtet sein.[565] Im folgenden Teil der Untersuchung werden in diesem Sinne

---

[562] Eine umfassende Übersicht über die Bedeutungsdimensionen des Begriffs „Jurisdiktion" in unterschiedlichen Kontexten ist in *Milanovic,* Extraterritorial Application of Human Rights Treaties, S. 19 ff. enthalten. Siehe dazu außerdem *Besson,* The Extraterritoriality of the European Convention on Human Rights. Siehe außerdem *Hildebrandt,* Extraterritorial Jurisdiction to Enforce in Cyberspace, S. 205 ff.

[563] Siehe Art. 2 Abs. 1 IPbpR, Art. 1 EMRK, Art. 1 Abs. 1 AMRK.

[564] *Milanovic,* Extraterritorial Application of Human Rights Treaties, S. 33, 53.

[565] So etwa auch der EGMR in *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 130: „The exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention".

die Jurisdiktionsklauseln im IPbpR und in der EMRK hinsichtlich der Frage beleuchtet, ob der Anwendungsbereich dieser Verträge allein mit dem Bestehen von „Jurisdiktion" eröffnet ist oder zusätzlich auf das eigene Staatsgebiet begrenzt ist. Eine extraterritoriale Anwendung der Pakte kommt nämlich nur in Betracht, wenn die Jurisdiktionsklausel keine territoriale Begrenzung des Anwendungsbereichs vorsehen. Entscheidend ist letztlich auch, wie weit oder eng der Menschenrechtsausschuss sowie der EGMR als zuständige Spruchkörper den Begriff der „Jurisdiktion" auslegen.

a. Die Jurisdiktionsklausel gemäß Art. 2 Abs. 1 IPbpR

Der Wortlaut des Art. 2 Abs. 1 IPbpR besagt, dass die Vertragsstaaten die Menschenrechte der im Staatsgebiet befindlichen und der Herrschaftsgewalt unterstehenden Individuen zu achten und zu gewährleisten haben:

> „1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Die Jurisdiktionsklausel des IPbpR umfasst damit sowohl den Begriff „*jurisdiction*" als auch „*territory*". Auf Grundlage des Wortlauts von Art. 2 Abs. 1 IPbpR und der Bezeichnung „*within its territory*" könnte somit die Schlussfolgerung gezogen werden, dass der Anwendungsbereich des IPbpR territorial an den Grenzen des jeweiligen Staatsgebiets endet.[566] Der Blick in die Entstehungsgeschichte des Paktes offenbart, dass tatsächlich die Formulierung des Art. 2 Abs. 1 IPbpR für Diskussionen gesorgt hat.[567] In den ersten Entwürfen des Vertragstextes war allein der Begriff „*jurisdiction*" vorhanden. Die Einfügung der Formulierung „*within its territory*" geht auf einen Entwurfsvorschlag der USA zurück.[568] Hintergrund dieses US-Entwurfs war die Besorgnis darüber, dass ohne die Ergänzung „*within ist territory*" eine Verpflichtung zur Gewährung der Menschenrechte gegenüber Personen in solchen Staaten, die unter der militärischen Besatzung der USA standen, entstehen würde.[569] Es sollte nach dieser von *Eleanor Roosevelt* vertretenen Sichtweise vermieden werden, den Vertragsstaaten Schutzpflichten für Gebiete aufzuerlegen, in denen ihnen gesetzgeberische

[566] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 4.11; *Johann,* Menschenrechte im internationalen bewaffneten Konflikt, S. 110.
[567] *Bossuyt,* Guide to the „Travaux Préparatoires", S. 53 ff.
[568] Ebd., S. 53. Siehe dazu UN Doc. E/CN.4/224, 23. Mai 1949: „The United States proposes that article 2 be revised to read as follows: ‚Each State party hereto undertakes to ensure to all individuals within its territory the rights set forth in this Covenant. […]'"; Siehe außerdem *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 23; *Dennis,* Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation, S. 123–124.
[569] UN Docs. E/CN.4/SR. 193, 26. Mai 1950, S. 13, 18.

Befugnisse fehlten.[570] Frankreich und andere Staaten plädierten wiederum dafür, „*territory*“ durch „*jurisdiction*“ zu ersetzen.[571] Sie argumentierten, dass ein Staat die Menschenrechte seiner Bürger sowohl im Ausland als auch im Inland gewährleisten müsse.[572] Schließlich wurde dennoch die Kombination beider Begriffe und damit die nun bestehende Fassung von Art. 2 Abs. 1 IPbpR angenommen.

Gerade der Wortlaut dieser Jurisdiktionsklausel hat zu unterschiedlichen Lesarten und Auslegungen geführt. Dementsprechend gehen die Ansichten über die extraterritoriale Anwendbarkeit des IPbpR auseinander. Im Folgenden sind einerseits die Ansichten des Menschenrechtsausschusses und des Internationalen Gerichtshofes, die eine extraterritoriale Anwendbarkeit des Paktes befürworten, sowie andererseits die Ansicht der Staaten, die eine extraterritoriale Geltung ablehnen, dargestellt.

aa. Die Spruchpraxis des MRA

Der Menschenrechtsausschuss hat seit jeher eine extraterritoriale Geltung des Paktes unter Art. 2 Abs.1 IPbpR befürwortet.[573] Nach der vom Ausschuss vertretenen Lesart ist das „*and*“ als ein „und/oder“ zu lesen, wonach die Begriffe „*territory*“ und „*jurisdiction*“ alternativ zueinander stehen.[574] Demzufolge ist ein Staat auch gegenüber Personen zur Achtung und Gewährleistung der Paktgarantien verpflichtet, die sich zwar nicht innerhalb des Territoriums des Staates befinden, aber unter der Hoheitsgewalt des Staates stehen.[575]

Bereits 1981 hat der Menschenrechtsausschuss in zwei Individualbeschwerden gegen Uruguay zur Auslegung von Art. 2 Abs. 1 IPbpR Stellung bezogen sowie das Bestehen extraterritorialer Verantwortung der Vertragsstaaten unter bestimmten Voraussetzungen begründet. In den Fällen *Lopez Burgos v. Uruguay*[576] und *Celiberti de*

[570] UN Docs. E/CN.4/SR. 193, 26. Mai 1950, S. 13, Rn. 53.

[571] *Bossuyt,* Guide to the „Travaux Préparatoires“, S. 54; Vgl. auch *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 35 ff.

[572] UN Docs. E/CN.4/SR. 193, 26. Mai 1950, S. 21. Als Vertreter Frankreichs argumentiert hier René Cassin das Wort „et“ durch „ou“ in dem französischen Entwurf zu ersetzen, mit folgender Begründung: „If that was not done many States would lose their jurisdiction over their foreign citizens.“ (Rn. 97).

[573] *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 4.11; UN Human Rights Committee, *Sergio Ruben Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981; UN Human Rights Committee, *Lilian Celiberti de Casariego v. Uruguay*, No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981.

[574] *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 67. Diese Lesart entspricht auch der überwiegenden Ansicht in der Literatur, siehe etwa *Buergenthal,* To Respect and to Ensure, in Henkin (Hrsg.), The International Bill of Rights, S. 74; *Johann,* Menschenrechte im internationalen bewaffneten Konflikt, S. 111.

[575] *Shany,* Taking Universality Seriously, S. 53; *Peters*, Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in Miller (Hrsg.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, S. 152 f.

[576] UN Human Rights Committee, *Sergio Ruben Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981.

Casariego v. Uruguay[577] wurden vermeintlich Oppositionelle aus Uruguay, die das Land verlassen und sich in Argentinien sowie Brasilien niedergelassen hatten, von uruguayischen Geheimdienstagenten im Ausland aufgespürt, festgenommen und anschließend heimlich nach Uruguay entführt. In Uruguay wurden sie schließlich inhaftiert, im Fall *Lopez Burgos v. Uruguay* zudem gefoltert. Der MRA stellte in beiden Fällen eine extraterritoriale Geltung des IPbpR fest. So habe Uruguay Paktbestimmungen verletzt, obwohl einige Verletzungshandlungen durch Uruguay auf fremden Staatsgebiet erfolgt sind. Weder Art. 2 Abs. 1 IPbpR noch Art. 1 des zweiten Zusatzprotokolls würden den Ausschuss davon ausschließen, eine extraterritoriale Verletzung der Paktbestimmungen festzustellen:

> „12.1 The Human Rights Committee further observes that although the arrest and initial detention and mistreatment of Lopez Burgos allegedly took place on foreign territory, the Committee is not barred either by virtue of article 1 of the Optional Protocol […] or by virtue of article 2 (1) of the Covenant […] from considering these allegations, together with the claim of subsequent abduction into Uruguayan territory, inasmuch as these acts were perpetrated by Uruguayan agents acting on foreign soil.“[578]

In der Begründung führt der Ausschuss aus, dass es nicht auf den Ort der Eingriffs- und Verletzungshandlung ankomme, sondern allein das Verhältnis zwischen dem Individuum und dem Staat hinsichtlich der geschehenen Menschenrechtsverletzung entscheidend sei:

> „12.2 The reference in article 1 of the Optional Protocol to ‚individuals subject to its jurisdiction' […] is not to the place where the violation occurred, but rather to the relationship between the individual and the State in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred.“[579]

Dabei legt der Ausschuss im Rahman dieser Beschwerden zwar nicht ausdrücklich fest, ob dieses Verhältnis faktischer oder rechtlicher Natur sein muss. Allerdings geht aus der Tatsache, dass in den beiden uruguayischen Fällen allein auf die Festnahme und Entführung abgestellt wird, hervor, dass nach Ansicht des Ausschusses durchaus rein faktische Handlungen diese Beziehung zwischen Individuum und Staat begründen können. Schließlich führt der Ausschuss eine ergebnisorientierte, an den Zweck des Paktes gestützte Argumentation an:

---

[577] UN Human Rights Committee, *Lilian Celiberti de Casariego v. Uruguay*, No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981.
[578] UN Human Rights Committee, *Sergio Ruben Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981, Rn. 12.1.
[579] Ebd., Rn. 12.2.

> „12.3 Article 2 (1) of the Covenant places an obligation upon a State party to respect and to ensure rights ‚to all individuals within its territory and subject to its jurisdiction', but it does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it. […]
>
> In line with this, it would be unconscionable to so interpret the responsibility under article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[580]

Hier bringt der Menschenrechtsausschuss damit deutlich zum Ausdruck, dass es den Staaten nicht zustehen kann, außerhalb ihres eigenen Territoriums Menschenrechtsverletzungen vorzunehmen, die ihnen innerhalb ihrer Staatsgrenzen aufgrund ihrer Verpflichtungen unter dem Pakt untersagt sind. Dabei ist die extraterritoriale Verantwortung der Staaten nicht davon abhängig, ob die Handlungen auf fremdem Territorium mit oder ohne Zustimmung der dortigen Regierung und somit rechtmäßig oder rechtswidrig erfolgen.[581]

Des Weiteren hat der Ausschuss auch in weiteren Individualbeschwerden, die grenzüberschreitende Staatshandlungen in unterschiedlichen Fallkonstellationen zum Gegenstand hatten, die extraterritoriale Anwendbarkeit des IPbpR befürwortet.[582] Im Jahr 2004 hat der Menschenrechtsausschuss zudem mit der Annahme des *General Comment* 31 seine bisherige Spruchpraxis zur extraterritorialen Anwendbarkeit des Paktes konkretisiert. So stellt der Ausschuss hier ausdrücklich fest, dass Art. 2 Abs. 1 IPbpR die Paktstaaten dazu verpflichte, die Rechte aller Personen, die sich entweder im Staatsgebiet oder unter der Hoheitsgewalt des Staates befinden, zu achten und zu gewährleisten.[583]

Auch in einer Reihe von *Concluding Observations* im Rahmen von Staatenberichtsverfahren hat der Menschenrechtsausschuss regelmäßig auf die extraterritoriale

[580] UN Human Rights Committee, *Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981, Rn. 12.1–12.3. Die gleiche Begründung des Menschenrechtsausschusses ist im Fall *Celiberti de Casariego v. Uruguay*, No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981, Rn. 10.1–10.3 zu finden.

[581] *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 51.

[582] Vgl. etwa UN Human Rights Committee, *Sophie Vidal Martins v. Uruguay*, No. 057/1979, CCPR/C/15/D/57/1979, 23. März 1982; *Samuel Lichtensztejn v. Uruguay*, No. 77/1980, CCPR/C/18/D/77/1980, 31. März 1983. Siehe außerdem *Nowak*, CCPR Commentary, Art. 2, S. 44, Rn. 30; *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 4.13 ff.

[583] UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004.

Anwendbarkeit des Paktes verwiesen und somit seine Position bekräftigt.[584] So bestätigte der Ausschuss beispielsweise die Anwendbarkeit des Paktes in den von Israel besetzen Territorien in Palästina:[585]

> „The Committee regrets that the State party continues to maintain its position on the non-applicability of the Covenant to the Occupied Territories, by claiming that the Covenant is a territorially bound treaty and does not apply with respect to individuals under its jurisdiction, but outside its territory, despite the interpretation to the contrary of article 2, paragraph 1, supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice (ICJ) and State practice. […] The State party should […] review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances, as outlined, inter alia, in the Committee's general comment No. 31 (2004) […]. In this respect, the Committee reiterates and underscores that the Covenant applies with regard to all conduct by the State party's authorities or agents adversely affecting the enjoyment of the rights enshrined in the Covenant by persons under its jurisdiction regardless of the location".[586]

bb. Die Auslegung des IGH

Der Internationale Gerichtshof hat den Standpunkt des Menschenrechtsausschusses in seinem Gutachten zur Rechtmäßigkeit der Errichtung einer Mauer in den von Israel besetzten palästinensischen Gebieten bestätigt.[587] Dabei verweist der IGH ausdrücklich auf die Entscheidungen *Lopez Burgos v. Uruguay*[588] und *Celiberti de Casariego v. Uruguay*[589] des Menschenrechtsausschusses. In seiner Argumentation stellt der Gerichtshof einerseits auf den Sinn und Zweck des IPbpR ab. So entspreche es dem Sinn und Zweck des Paktes, dass die Staaten auch bei extraterritorialen Hoheitsakten an ihre aus dem IPbpR hervorgehenden Verpflichtungen gebunden

[584] Siehe beispielsweise UN Human Rights Committee, Concluding observations: Yugoslavia, CCPR/C/79/Add. 16, 28. Dezember 1992, Rn. 7; Concluding observations: Netherlands, CCPR/CO/72/NET, 27. August 2001, Rn. 8, 27; Concluding observations: Belgium, CCPR/CO/81/BEL, 12. August 2004, Rn. 6; Concluding observations: USA, CCPR/C/USA/CO/3/Rev. 1, 18. Dezember 2006, Rn. 10.

[585] Vgl. auch *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 4.12.

[586] UN Human Rights Committee, Concluding observations: Israel, CCPR/C/ISR/CO/4, 21. November 2014, Rn. 5.

[587] International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136.

[588] UN Human Rights Committee, *Sergio Ruben Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981.

[589] UN Human Rights Committee, *Lilian Celiberti de Casariego v. Uruguay,* No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981.

seien.[590] Des Weiteren verweist der IGH auch auf die Entstehungsgeschichte des Wortlauts von Art. 2 Abs. 1 IPbpR:

> „The travaux préparatoires of the Covenant confirm the Committee's interpretation of Article 2 of that instrument. These show that, in adopting the wording chosen, the drafters of the Covenant did not intend to allow States to escape from their obligations when they exercise jurisdiction outside their national territory. They only intended to prevent persons residing abroad from asserting, vis-à-vis their State of origin, rights that do not fall within the competence of that State, but of that of the State of residence."[591]

Damit stellt der Gerichtshof letztlich fest, dass die vom Menschenrechtsausschuss vertretene Auffassung korrekt ist und der IPbpR auch bei staatlicher Ausübung von Jurisdiktion außerhalb des Staatsterritoriums anwendbar ist.[592] Diesen Standpunkt hat der IGH zudem in seinem verbindlichen Urteil im Fall *Democratic Republic of the Congo v. Uganda* (*DRC v. Uganda*) zur Frage der Verantwortlichkeit Ugandas für die von seinen Soldaten im Kongo verübten Menschenrechtsverletzungen bestätigt. Dabei verwies der Gerichtshof auf seine Argumentation im *Wall*-Gutachten.[593]

Damit hat der IGH, das als Hauptrechtsprechungsorgan der UN in der Weltgemeinschaft hohe Anerkennung genießt, die Sichtweise des Menschenrechtsausschusses hinsichtlich der Auslegung des Art. 2 Abs. 1 IPbpR erheblich gestärkt. Die Stellungnahme des Gerichtshofs im *Wall*-Gutachten und seine Sichtweise im völkerrechtlich verbindlichen Urteil *DRC v. Uganda* untermauert zweifelsfrei die Spruchpraxis des Menschenrechtsausschusses hinsichtlich der extraterritorialen Anwendbarkeit des IPbpR.[594]

---

[590] International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136, Rn. 109

[591] International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136, Rn. 109. Nach der entgegengesetzten Ansicht von Nowak offenbare die Entstehungsgeschichte vielmehr, dass die Staaten mit der abschließenden Annahme des Wortlauts gerade eine Verpflichtung der Staaten gegenüber Personen, die sich zwar unter der Jurisdiktion eines Staates, aber außerhalb des Territoriums befinden, vermeiden wollten. Siehe *Nowak*, CCPR Commentary, Art. 2, S. 43, Rn. 27. Im Ergebnis befürwortet aber auch Nowak mit Verweis auf den Sinn und Zweck der Norm die extraterritoriale Anwendbarkeit des Paktes, vgl. ebd., S. 44, Rn. 29. Allerdings wird gerade die Entstehungsgeschichte insbesondere von den USA als Kernargument gegen eine extraterritoriale Anwendbarkeit des Paktes angeführt, siehe dazu nachfolgenden Unterabschnitt A. I. 1. a. cc.

[592] International Court of Justice, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136, Rn. 109, Rn. 111.

[593] International Court of Justice, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, 19. Dezember 2005, I.C.J. Reports 2005, S.168, Rn. 216.

[594] So auch *Wilde,* Human Rights beyond Borders at the World Court, S. 666.

cc. Die Staatenpraxis

Unter Bezugnahme auf den Wortlaut und der Entstehungsgeschichte des Art. 2 I IPbpR haben die USA, aber etwa auch Israel und die Niederlande, den Standpunkt eingenommen, dass eine extraterritoriale Anwendbarkeit des Paktes ausgeschlossen sei und die Vertragsstaaten nur für Handlungen innerhalb des eigenen Territoriums verantwortlich seien.[595] Auch haben in den Anfangsjahren des Aufkeimens dieser Debatte in Wissenschaftskreisen erste Literaturstimmen diesen Standpunkt vertreten.[596] So ist nach dieser Ansicht die Konjunktion „*and*" als kumulative Verbindung der beiden Satzteile „*within ist territory*" sowie „*subject to its jurisdiction*" zu verstehen. Demnach sei der IPbpR nur für Personen anwendbar, die sich sowohl innerhalb des Staatsgebiets befinden und zudem unter der Jurisdiktion des Staates stehen.[597] Die USA verweisen zudem auf die *travaux préparatoires*, aus denen hervorgehe, dass die Staaten den Geltungsbereich des Paktes auf das Staatsgebiet begrenzen wollten.[598]

---

[595] Während des Dialogs mit dem Menschenrechtsausschuss zum ersten Staatenbericht der USA unter Art. 40 I IPbpR im Jahr 1995 hat die US-Delegation erstmals ausdrücklich diesen Standpunkt artikuliert. UN Human Rights Committee, Summary Records of the 1405th Meeting, CCPR/C/SR.1405, 24 April 1995, Rn. 20: „Mr. Klein had asked whether the United States took the view that the Covenant did not apply to government actions outside the United States. The Covenant was not regarded as having extraterritorial application. In general, where the scope of application of a treaty was not specified, it was presumed to apply only within a party's territory. Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized ‚to all individuals within its territory and subject to its jurisdiction'. That dual requirement restricted the scope of the Covenant to persons under United States jurisdiction and within United States territory. During the negotiating history, the words ‚within its territory' had been debated and were added by vote, with the clear understanding that such wording would limit the obligations to within a Party's territory." Diesen Standpunkt vertreten die USA auch weiterhin. Siehe dazu Fifth Periodic Report USA vom 11. November 2021, CCPR/C/USA/5, Rn. 14. Vgl. auch *Shaack,* The United States' Position on the Extraterritorial Application of Human Rights Obligations, S. 53 ff. Israel vertritt auch den Standpunkt, dass die Voraussetzungen des Art. 2 Abs. 1 IPbpR kumulativ vorliegen müssen. Aus diesem Grund gelte nach Ansicht Israels der IPbpR auch nicht in den besetzten palästinensischen Territorien. Siehe dazu etwa Fourth Periodic Report Israel vom 12. Dezember 2013, CCPR/C/ISR/4, Rn. 48 sowie Fifth Periodic Report vom 30. Oktober 2019, C CPR/C/ISR/5, Rn. 22–25. Die Niederlande lehnen die Anwendbarkeit des Paktes hinsichtlich des Verhaltens ihrer Blauhelmsoldaten im Fall des Massenmordes von Zivilpersonen in Srebrenica (Bosnien 1995) mit Verweis auf den Wortlaut des Art. 2 Abs. 1 IPbpR ab. Vgl. Follow-up State party's report, Replies of the Government of the Netherlands to the concerns expressed by the Human Rights Committee in its concluding observations (CCPR/CO/72/NET), CCPR/CO/72/NET/Add. 1, Rn. 19.

[596] *Nowak*, The Effectiveness of the International Covenant on Civil and Political Rights, S. 156; *Schwelb,* Civil and Political Rights, S. 863. Vgl. außerdem *Dennis,* Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation, S. 122.

[597] Näheres zur Argumentation dieser Ansicht siehe *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 66–67.

[598] Siehe etwa United States of America third periodic report to the Human Rights Committee, CCPR/C/USA/3, Annex I, 28. November 20015, p. 110: „The preparatory work of the Covenant establishes that the reference to ‚within its territory' was included within Article 2(1) of the Covenant

Im Rahmen des *Wall*-Gutachtenverfahrens des IGH haben jedoch eine Vielzahl von Staaten in ihren Stellungnahmen festgestellt, dass der Pakt auch in den besetzten Gebieten Anwendung findet und damit die extraterritoriale Anwendbarkeit des IPbpR im Grundsatz eindeutig bejaht.[599] Auch im Rahmen der Staatenberichtsverfahren vor dem Menschenrechtsausschuss ist diese Position der überwiegenden Mehrheit der Staaten erkennbar.[600] Daraus lässt sich durchaus folgern, dass die Befürwortung der extraterritorialen Anwendbarkeit des Paktes und die Auslegung des Art. 2 Abs. 1 IPbpR im Sinne der Lesart des Ausschusses – trotz der dargelegten Gegenpositionen seitens weniger Staaten – der überwiegenden Staatenpraxis entspricht.[601] Hiervon geht offenbar auch der Menschenrechtsausschuss selbst aus, denn in den oben zitierten *Concluding Observations* für Israel bezeichnete er seine Interpretation des Art. 2 Abs. 1 IPbpR als allgemeine Staatenpraxis.[602] Dieser Umstand ist nach Art. 31 Abs. 3 lit. b der Wiener Vertragsrechtskonvention[603] für die Auslegung des Art. 2 Abs. 1 IPbpR zu berücksichtigen.

dd. Würdigung und Ergebnis

Der Wortlaut von Art. 2 Abs. 1 IPbpR gibt tatsächlich nicht eindeutig vor, wie die Begriffe „*jurisdiction*“ und „*territory*“ zueinander stehen und lässt dadurch unterschiedliche Interpretationen zu. Einer extraterritorialen Anwendung des Paktes steht der Wortlaut insofern auch nicht entgegen. Im Sinne des Art. 31 Abs. 1 der WVRK[604] ist es in diesem Fall geboten, Art. 2 Abs. 1 IPbpR im Lichte seines Zieles und Zwecks auszulegen. Die Jurisdiktionsklausel definiert die menschenrechtliche Verpflichtung der Staaten, die Ihnen als Mitglied dieses Paktes obliegt. Die Präambel des IPbpR zeigt dabei, dass eine enge Eingrenzung der staatlichen Pflichten

---

to make clear that states would not be obligated to ensure the rights recognized therein outside their territories.“ Dabei berufen sich die USA auf die Äußerungen der Vertreterin der US-Delegation, Eleanor Roosevelt, während der Entwurfssitzungen: „That amendment was designed to make clear that the covenant was applicable only to persons within the territory and jurisdiction of the contracting parties. Otherwise it could be interpreted as obliging a contracting party to adopt legislation applying to persons outside its territory although technically within its jurisdiction for certain questions. That would be the case, for example, in the occupied territories of Germany, Austria and Japan, as persons living in those territories were in certain respects subject to the jurisdiction of the occupying Powers but were in fact outside the legislative sphere of those Powers.“ Siehe UN Doc. E/CN.4/SR. 193, 26. Mai 1950, S. 13.

[599] Siehe dazu *Johann,* Menschenrechte im internationalen bewaffneten Konflikt, S. 114 f., Fn. 159 mit ausführlichen Verweisen.

[600] Siehe Ebd., S. 113; *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 90.

[601] So auch *Johann,* Menschenrechte im internationalen bewaffneten Konflikt, S. 113.

[602] UN Human Rights Committee, Concluding observations: Israel, CCPR/C/ISR/CO/4, 21. November 2014, Rn. 5.

[603] Im Folgenden: „WVRK“.

[604] Art. 31 Abs. 1 WVRK: „A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.“

nicht Ziel der Jurisdiktionsklausel sein kann. Art. 2 Abs. 1 IPbpR ist im Zusammenhang mit der Präambel zu lesen und auszulegen. In der Präambel wird die Anerkennung der Würde und Gleichheit aller Mitglieder der menschlichen Gesellschaft als Grundsatz des Paktes verankert. Die Auslegung der Jurisdiktionsklausel des IPbpR darf in diesem Sinne nicht dazu führen, dass außerhalb des Staatsgebiets Menschenrechtsverstöße durchgeführt werden dürfen. Eine rein territoriale Auslegung des Art. 2 Abs. 1 IPbpR hätte dieses Ergebnis zur Folge. Dies würde eklatant mit dem Wesen des internationalen Menschenrechtsschutzes und seinem Universalitätsanspruch in Widerspruch stehen. Aus der Präambel des IPbpR geht der universelle Geltungsbereich der kodifizierten Menschenrechte eindeutig hervor:

> „The States Parties to the present Covenant, […] Considering the obligation of States under the Charter of the United Nations to promote universal respect for, and observance of, human rights and freedoms, […] Agree upon the following articles".

Dies entspricht auch der Argumentation des MRA, der einen ergebnisorientierten Auslegungsansatz zugrunde legt. In diesem Sinne ist der Ansicht des MRA sowie des IGH und der allgemeinen Staatenpraxis zuzustimmen. Art. 2 Abs. 1 IPbpR ist demzufolge nach hier vertretener Auffassung so auszulegen, dass die Paktstaaten auch gegenüber Individuen außerhalb des Staatsgebiets zur Achtung der Paktgarantien verpflichtet sind, die sich unter der Hoheitsgewalt des Staates befinden.

b. Die Jurisdiktionsklausel gemäß Art. 1 EMRK im Lichte der Spruchpraxis des EGMR

Gemäß Art. 1 EMRK sind die Mitgliedstaaten dazu verpflichtet, gegenüber allen Personen, die unter der Hoheitsgewalt des Staates stehen, die Konventionsrechte zu sichern:

> „The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."

Im Gegensatz zum IPbpR enthält der Wortlaut des Art. 1 EMRK, der den Anwendungsbereich der Konvention normiert, somit keinen territorialen Bezug. Die Auslegung des Begriffs „*jurisdiction*" und die Frage, unter welchen Voraussetzungen Staaten Hoheitsgewalt im Sinne des Art. 1 EMRK ausüben, waren Gegenstand mehrerer Fälle vor dem EGMR. Bereits die EKMR hat sich schon früh mit der Auslegung von Art. 1 EMRK in einschlägigen Fällen befassen müssen und dabei die extraterritoriale Anwendbarkeit des Paktes im Grundsatz befürwortet.[605] Der

[605] EKMR, *X. v. The Federal Republic of Germany,* Rs. 1611/62, 25. September 1965, Yearbook 8, S. 158 (S. 168); *Hess v. the United Kingdom*, Rs. 6231/73, 28 May 1975, D.R. 2, S. 72 (S. 73 f.); *Cyprus v.*

EGMR hat in seiner frühen einschlägigen Rechtsprechung auf die Ansichten der EKMR verwiesen und festgestellt, dass der Begriff „*jursidiction*" in Art. 1 EMRK nicht auf die Territorien der Konventionsstaaten begrenzt sei. So könnten Staaten auch für solche Handlungen verantwortlich sein, die außerhalb ihres eigenen Staatsgebiets Auswirkungen haben.[606]

aa. Der Fall Loizidou v. Turkey

Die erste wichtige Leitentscheidung des EGMR zur Auslegung des Begriffs „*jurisdiction*" und der extraterritorialen Anwendbarkeit der Konvention erging im Fall *Loizidou v. Turkey*.[607] Die griechisch-zypriotische Beschwerdeführerin dieses Falles machte eine Verletzung von Art. 8 EMRK und Art. 1 des ersten Zusatzprotokolls der EMRK[608] durch die Türkei geltend, da ihr der Zugang zu ihren Grundstücken in Nordzypern seit der Besetzung dieses Landesteils durch die Türkei verwehrt wurde und sie somit an der Ausübung ihrer Eigentumsrechte verhindert worden war. Der EGMR hat dabei zunächst in einem gesonderten Urteil zu den Vorabeinreden der Türkei untersucht, inwieweit die von der Beschwerdeführerin beklagten Handlungen in die Hoheitsgewalt der Türkei fielen, obwohl die Handlungen außerhalb des türkischen Staatsgebiets erfolgten.[609] So hat die Türkei vorab den Einwand erhoben, dass der EGMR *ratione loci* unzuständig sei. In diesem Urteil stellt der EGMR ausdrücklich fest, dass „*jursidiction*" im Sinne des Art. 1 Abs. 1 EMRK keineswegs auf das Staatsgebiet der Vertragsstaaten begrenzt ist.[610] Aus dem Sinn und Zweck der Konvention sei zu schließen, dass die Verantwortlichkeit der Staaten auch dann bestehen müsse, wenn diese infolge von militärischen Operationen

---

Turkey, Rs. 6780/74 und 6950/75, 26. Mai 1975, D.R.2, S. 125 (S. 136 f.); *X and Y v. Switzerland,* Rs. 7289/75 und 7349/76, 14. Juli 1977, D.R. 9, S. 57 (S. 71); *W. v. the United Kingdom*, Rs. 9348/81, 28. Februar 1983, D.R. 32, S. 190.

[606] EGMR, *Drozd and Janousek v. France and Spain*, Rs. 12747/87, 26. Juni 1992, Serie A 240, Rn. 91. Der EGMR verweist hier auf die in Fn. 573 genannten Entscheidungen der EKMR.

[607] Mit dem Fall *Loizidou v. Turkey* befasste sich zunächst die EKMR, siehe Bericht der EKMR, *Loizidou v. Turkey*, Rs. 15318/89, 8. Juli 1993, Serie A 310. In einem Urteil zu den Vorabeinreden prüfte der EGMR anschließend die Einrede der Türkei, wonach der Gerichtshof *ratione loci* unzuständig sei, siehe EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Preliminary Objections), 23. März 1995, Serie A 310. Schließlich erging 1996 das Urteil des EGMR zur Begründetheit, vgl. EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI.

[608] Art. 1 des ersten Zusatzprotokolls lautet:
„1. Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
2. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

[609] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Preliminary Objections), 23. März 1995, Serie A 310.

[610] Ebd., Rn. 62.

effektive Kontrolle („*effective control*") über fremdes Gebiet ausüben.[611] Im Ergebnis hat der Gerichtshof im Urteil über die Vorabeinreden festgestellt, dass die gerügte Zugangsverweigerung zu den Grundstücken in die Hoheitsgewalt der Türkei fiel. Im anschließend 1996 ergangenen Urteil zur Begründetheit des Falles *Loizidou v. Turkey* hat der EGMR dieses Ergebnis bestätigt und die wesentlichen Argumente für das Urteil zur Begründetheit hervorgehoben.[612] Auf Grundlage der effektiven Kontrolle infolge militärischer Operationen auf fremden Territorien seien demnach die Vertragsstaaten zur Sicherstellung der Konventionsrechte auf diesen Gebieten verpflichtet, und zwar unabhängig davon, ob diese direkt durch eigene Streitkräfte oder durch eine nachgeordnete Lokalverwaltung ausgeübt wird.[613] Des Weiteren hebt der EGMR hervor, dass der von der Beschwerdeführerin gerügte Verlust der Ausübung ihrer Eigentumsrechte auf die Besetzung des nordzypriotischen Landesteils durch die Türkei und die Gründung der „TRNC"[614] zurückzuführen sei.[615] Zudem hätten die türkischen Truppen der Beschwerdeführerin den Zugang zu ihren Grundstücken verwehrt.[616] Dass die Türkei über den nordzypriotischen Landesteil effektive Gesamtkontrolle („*effective overall control*") ausübe, sei dem Gerichtshof zufolge eindeutig:

> „It is obvious from the large number of troops engaged in active duties in northern Cyprus […] that her army exercises effective overall control over that part of the island. Such control […] entails her responsibility for the policies and actions of the ‚TRNC' […]. Those affected by such policies or actions therefore come within the ‚jurisdiction' of Turkey for the purposes of Article 1 of the Convention (art. 1). Her obligation to secure to the applicant the rights and freedoms set out in the Convention therefore extends to the northern part of Cyprus."[617]

Damit stellt der Gerichtshof abschließend fest, dass die wiederholte Zugangsverweigerung zu den nordzypriotischen Grundstücken und der infolgedessen erlittene Verlust der Ausübung von Eigentumsrechten durch die Beschwerdeführerin

[611] Ebd., Rn. 62.
[612] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI.
[613] Ebd., Rn. 52.
[614] „TRNC" steht für Turkish Republic of Northern Cyprus (Türkische Republik Nordzypern).
[615] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI, Rn. 54.
[616] Ebd.
[617] Ebd., Rn. 56. *Thallinger* hebt in diesem Zusammenhang hervor, dass der EGMR in dieser Entscheidung mit der Formel „*effective overall control*" letztlich den im Bericht der EKMR zur Rechtssache *Loizidou v. Turkey* gewählten Begriff „*overall control*" und der im EGMR-Urteil zu den Vorabeinreden genannten Formulierung „*effective control*" kombiniert. Vgl. *Thallinger*, Grundrechte und extraterritoriale Hoheitsakte, S. 122.

allesamt in die Jurisdiktion der Türkei im Sinne des Art. 1 Abs. 1 EMRK fallen.[618] Der EGMR stellt im Fall *Loizidou v. Turkey* somit in aller Deutlichkeit fest, dass eine extraterritoriale Anwendbarkeit der Konvention von Art. 1 EMRK umfasst ist. Im Rahmen dieser Entscheidung stellen die Straßburger Richter auf die effektive Gesamtkontrolle über Territorien aufgrund militärischer Operationen ab und begründen damit das Vorliegen der Jurisdiktion eines Staates.

Mit Verweis auf die Entscheidung *Loizidou v. Turkey* bestätigt der EGMR auch in der Staatenbeschwerde *Cyprus v. Turkey*, dass die Türkei in Nordzypern effektive Gesamtkontrolle („*effective overall control*") verfügt.[619] Damit sei die Türkei im Sinne des Art. 1 Abs. 1 EMRK für die Handlungen eigener Streitkräfte und Beamte vor Ort, aber auch für die Handlungen der Lokalverwaltung, die letztlich aufgrund der militärischen Unterstützung durch die türkischen Truppen aufrecht erhalten werde, verantwortlich.[620]

bb. Der Fall Banković and Others v. Belgium and Others

Der EGMR führt in seiner nachfolgenden Rechtsprechung indes diese weite Auslegung des Jurisdiktionsbegriffs in Art. 1 EMRK nicht fort. Vielmehr begründet der EGMR in der 2001 ergangenen Entscheidung *Banković and Others v. Belgium and Others*[621] einen engen Jurisdiktionsbegriff.[622] Hintergrund dieser Entscheidung ist der Einsatz der NATO während des Kosovo-Konflikts im Jahr 1999. Während der Luftangriffe durch die NATO im April 1999 wurde ein Gebäude der Radio- und Fernsehstation RTS in Belgrad bombardiert, wobei 16 Todesopfer und weitere 16 Schwerverletzte die Folge waren. Die jugoslawischen Beschwerdeführer, die entweder selbst durch die Bombardierung verletzt wurden oder Angehörige der Opfer sind, beklagten eine Verletzung der Art. 2, 10 und 13 EMRK durch die Staaten, die in dem NATO-Einsatz involviert waren. Dabei machen sie unter Bezugnahme auf die vorangegangene Spruchpraxis des Gerichtshofs geltend, dass die Bombardierung sowie die Tötungen und Verletzungen der Opfer unter die Jurisdiktion der agierenden Staaten fielen und diese demnach proportional zum Umfang ihrer

[618] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI, Rn. 57.
[619] EGMR, *Cyprus v. Turkey* [GC], Rs. 25781/94, 10. Mai 2001, Rep. 2001-IV, Rn. 77. Zuvor hatte sich die EKMR bereits mit zwei weiteren Staatenbeschwerden Zyperns gegen die Türkei befasst und dabei festgestellt, dass die Jurisdiktion eines Staates im Sinne des Art. 1 Abs. 1 EMRK nicht an den territorialen Grenzen des Staatsgebiets gebunden ist. Siehe EKMR, *Cyprus v. Turkey*, Rs. 6780/74 und 6950/75, 26. Mai 1975, D.R.2, S. 125; EKMR, *Cyprus v. Turkey*, Rs. 8007/77, 10. Juli 1978, D.R.13, S. 85.
[620] EGMR, *Cyprus v. Turkey* [GC], Rs. 25781/94, 10. Mai 2001, Rep. 2001-IV, Rn. 77.
[621] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII.
[622] Vgl. auch *Thallinger*, Grundrechte und extraterritoriale Hoheitsakte, S. 125.

Kontrolle zur Sicherung der Konventionsrechte gemäß Art. 1 EMRK verpflichtet seien.[623]

Der EGMR befasst sich in dieser Entscheidung eingehend mit der Frage, inwieweit in Art. 1 EMRK extraterritoriale Verpflichtungen der Vertragsstaaten niedergelegt sind. Dazu legt er zunächst die Formulierung „*within their jurisdiction*" im Lichte der völkerrechtlichen Auslegungsregeln gemäß Art. 31 und 32 der Wiener Vertragsrechtskonvention aus und stellt im Ergebnis fest, dass dem Begriff „*jurisdiction*" grundsätzlich eine territoriale Bedeutung zukomme.[624] Demnach werde Jurisdiktion vorrangig auf dem territorialen Hoheitsgebiet eines Staates ausgeübt und nur in einzelnen Ausnahmefällen komme eine extraterritoriale Hoheitsgewalt in Betracht:

> „61. The Court is of the view, therefore, that Article 1 of the Convention must be considered to reflect this ordinary and essentially territorial notion of jurisdiction, other bases of jurisdiction being exceptional and requiring special justification in the particular circumstances of each case. […]
>
> 67. In keeping with the essentially territorial notion of jurisdiction, the Court has accepted only in exceptional cases that acts of the Contracting States performed, or producing effects, outside their territories can constitute an exercise of jurisdiction by them within the meaning of Article 1 of the Convention."[625]

Der Gerichtshof legt hier folglich eine restriktive Auslegung des Jurisdiktionsbegriffs gemäß Art. 1 Abs. 1 EMRK zugrunde und stellt damit die extraterritoriale Anwendbarkeit der Konvention als einen Ausnahmefall dar. Damit stellt der Gerichtshof hier erstmals eine Regel-Ausnahme-Formel auf und begründet einen territorialen Jurisdiktionsbegriff.[626] Denn in den Entscheidungen vor *Banković*, – insbesondere aber in der Leitentscheidung *Loizidou* – hat der Gerichtshof vielmehr festgestellt, dass „*jursidiction*" eben nicht auf das Staatsgebiet der Vertragsstaaten begrenzt ist. Die extraterritoriale Jurisdiktion wurde in diesen Entscheidungen keineswegs ausdrücklich als Ausnahme definiert. Dennoch zieht der Gerichtshof im *Banković*-Urteil seine bisherige Spruchpraxis als bestätigendes Argument für die Regel-Ausnahme-Formel heran:

---

[623] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 46 ff.

[624] Dazu legt der EGMR nicht nur den Wortlaut des Art. 1 Abs. 1 EMRK aus, sondern zieht zudem die bisherige Staatenpraxis sowie die Entstehungsgeschichte (*travaux préparatoires*) heran. EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 59 ff.

[625] Ebd., Rn. 61 und 67.

[626] Vgl. auch *Shany,* Taking Universality Seriously, S. 57.

> „In sum, the case-law of the Court demonstrates that its recognition of the exercise of extra-territorial jurisdiction by a Contracting State is exceptional: it has done so when the respondent State, through the effective control of the relevant territory and its inhabitants abroad as a consequence of military occupation or through the consent, invitation or acquiescence of the Government of that territory, exercises all or some of the public powers normally to be exercised by that Government.“[627]

Weiterhin stellt der Gerichtshof fest, dass die EMRK als regionales Instrument innerhalb des europäischen Rechtsraums (*espace juridique*) Geltung entfalte und nicht für eine weltweite Anwendung vorgesehen sei, selbst wenn die Vertragsstaaten weltweit handelten. Die Föderative Volksrepublik Jugoslawien, die zum Zeitpunkt der Bombardierungen kein Mitgliedstaat der EMRK war, sei dem Gerichtshof zufolge somit nicht vom besagten Rechtsraum erfasst. Daraus folgern die Straßburger Richter schließlich, dass die Nichtanwendung der Konvention in diesem konkreten Fall kein Vakuum im Menschenrechtsschutz der EMRK begründet.[628] Des Weiteren lehnt der Gerichtshof in dem *Banković*-Urteil eine „*cause-and-effect*“ Jurisdiktion ab, sodass durch isolierte Rechtsverletzungen im Ausland keine zugeschnittene Jurisdiktion begründet werden könne.[629] Gestützt auf diesen Argumenten verneinte der EGMR im Ergebnis die Jurisdiktion der involvierten NATO-Staaten.

Die *Banković*-Entscheidung hat insbesondere in Wissenschaftskreisen kontroverse Diskussionen und beachtliche Kritik ausgelöst.[630] Insbesondere führe die *espace-juridique*-Argumentation des Gerichtshofs den Kritikern zufolge zu absurden, mit Kernprinzipien des internationalen Menschenrechtsschutzes unvereinbaren Ergebnissen. Dieser Kritik ist durchaus zuzustimmen. Denn die Argumentation des EGMR hätte zur Folge, dass die Konventionsstaaten im Ausland – außerhalb des Geltungsbereiches der Konvention – menschenrechtsverletzende Handlungen vornehmen dürften, die innerhalb ihrer eigenen Grenzen konventionswidrig wären.

---

[627] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 71.

[628] Ebd., Rn. 80.

[629] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 75; *Medvedyev and Others v. France,* Rs. 3394/03, 29. März 2010, Rep. 2010, Rn. 64. Vgl. auch *Rooney*, The Relationship between Jurisdiction and Attribution after Jaloud v. Netherlands, S. 419.

[630] Siehe beispielsweise *De Schutter,* Globalization and Jurisdiction. Lessons from the European Convention on Human Rights, S. 191 ff.; *Orakhelashvili,* Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights, S. 538 ff.; *Wilde:* State Obligations Extraterritorially, S. 505 ff; *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 123 f.

cc. *Post-Banković*-Rechtsprechung

In den darauffolgenden Jahren hat der EGMR zwar die Regel-Ausnahme-Formel beibehalten, allerdings wird aus der *Post-Banković*-Rechtsprechung deutlich, dass der Gerichtshof allmählich von seiner restriktiven Sichtweise im *Banković*-Urteil abgerückt ist.

In der Entscheidung *Öcalan v. Turkey*[631] hat der Gerichtshof erstmals festgestellt, dass ein Staat auch punktuell extraterritoriale Jurisdiktion über eine Person, die unter seiner Gewalt und Kontrolle („*authority and control*") steht, ausüben kann, ohne dass eine territoriale Kontrolle über das entsprechende Gebiet bestehen muss.[632] Zwar legt der EGMR im Rahmen dieser Entscheidung seine Feststellungen aus *Banković* ausdrücklich zugrunde.[633] Ausgehend von der Regel-Ausnahme-Formel erkennt hier der Gerichtshof jedoch die punktuelle, personenbezogene Jurisdiktion immerhin als einen weiteren exzeptionellen Anwendungsfall für die extraterritoriale Anwendbarkeit der Konvention an. Dabei sei an dieser Stelle angemerkt, dass der EGMR im Fall *Banković* nicht einmal die Frage ausdrücklich aufgeworfen hat, ob das Bombardement und die Tötung der Personen aufgrund personeller Kontrolle die Jurisdiktion der involvierten Staaten begründet hat.[634] Beachtlich ist aber insbesondere, dass der EGMR im Fall *Öcalan v. Turkey* offenbar mit der in *Banković* strikt formulierten *espace-juridique*-Argumentation bricht.[635] Denn immerhin steht offenbar die Tatsache, dass die extraterritoriale Handlung dieses Falles außerhalb des EMRK-Gebiets stattfand, der Feststellung der Jurisdiktion im Sinne des Art. 1 EMRK nicht im Wege.

In der Entscheidung *Issa and Others v. Turkey* hat der Gerichtshof zwar im Ergebnis angesichts der konkreten Fallumstände das Vorliegen von Jurisdiktion verneint.[636] Dennoch offenbaren die Ausführungen in diesem Urteil nennenswerte Entwicklungen in der Spruchpraxis des EGMR hinsichtlich der extraterritorialen Anwendbarkeit der Konvention. So bestätigt der Gerichtshof die personelle Kontrolle von Individuen im Sinne der „*authority and control*"-Doktrin als Jurisdiktions-Fallgruppe.[637] Dabei verweisen die Straßburger Richter interessanterweise auf die

---

[631] EGMR, *Öcalan v. Turkey*, Rs. 46221/99, 12. März 2003, dieses Urteil wurde von der Großen Kammer im Ergebnis bestätigt: EGMR, *Öcalan v. Turkey* [GC], Rs. 46221/99, 12. Mai 2005, Rep. 2005-IV. Dieser Fall handelt von der Festnahme des PKK-Führers Öcalan durch türkische Beamte in Nairobi, Kenia.

[632] EGMR, *Öcalan v. Turkey* [GC], Rs. 46221/99, 12. Mai 2005, Rep. 2005-IV, Rn. 91.

[633] EGMR, *Öcalan v. Turkey*, Rs. 46221/99, 12. März 2003, Rn. 93

[634] So auch *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 123.

[635] Vgl. *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 164.

[636] EGMR, *Issa and Others v. Turkey*, 31821/96, 16. November 2004, Rn. 72 ff. Dieser Fall betraf eine Militäraktion der Türkei im Nordirak und die Tötung von irakischen Schafhirten auf dem betroffenen Gebiet. Die Beschwerdeführer konnten indes nicht beweisen, dass die Tötung durch türkische Soldaten erfolgte.

[637] EGMR, *Issa and Others v. Turkey*, 31821/96, 16. November 2004, Rn. 71.

Entscheidungen *Lopez Burgos v. Uruguay*[638] und *Celiberti de Casariego v. Uruguay*[639] des UN-Menschenrechtsausschuss und zitieren dabei fast wörtlich die Argumentation des Ausschusses:

> „Accountability in such situations stems from the fact that Article 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory."[640]

Damit distanziert sich der EGMR nun noch deutlicher von der im *Banković*-Entscheid vertretenen strikten *espace-juridique*-Doktrin.[641] So bringt der Gerichtshof hiermit nämlich zum Ausdruck, dass die Schaffung eines europäischen Rechtsraums durch die EMRK keineswegs die Staaten davon entbindet, auch außerhalb ihres Territoriums und des regionalen Rechtsraums ihre Konventionsverpflichtungen zu achten. Zwar gibt der Gerichthof die *espace-juridique*-Doktrin im Grundsatz nicht auf, stellt aber richtigerweise fest, dass diese im Ergebnis keinen Freibrief für extraterritoriale Menschenrechtsverletzungen darstellen dürfe.

Ein wichtiger Grundpfeiler in der *Post-Banković*-Rechtsprechung des Gerichtshofes ist indes die Entscheidung *Al-Skeini and Others v. The United Kingdom*.[642] Beschwerdeführer dieses Falles waren die Angehörigen von sechs irakischen Zivilisten, die während des Irak-Einsatzes 2003 von britischen Soldaten in Basra getötet wurden. Während eines der Todesopfer nach einem Verhör in britischer Haft ums Leben gekommen war, wurden die anderen Personen während Hausdurchsuchungen, Feuergefechten und Patrouillen durch britische Soldaten in Basra erschossen. Ein Todesopfer wurde zudem nach Androhung von Waffengewalt durch britische Soldaten in einen Fluss gestoßen und später dort tot aufgefunden.[643] Im Fall des Verhöropfers wurde eine unabhängige Untersuchung durchgeführt. In allen anderen Fällen fanden nur eingeschränkte Untersuchungen durch britische Militärbehörden statt. Unter Berufung auf Art. 2 EMRK machten die Beschwerdeführer geltend, dass das Vereinigte Königreich seine prozessualen Ermittlungspflichten – außer im Falle des Verhöropfers – verletzt habe.[644]

Der EGMR musste also auch im Fall *Al-Skeini* zunächst prüfen, ob die Todesopfer der Jurisdiktion des Vereinigten Königreichs unterstanden. Dabei stellt der Gerichtshof auch hier zunächst allgemein heraus, dass „*jurisdiction*" im Sinne des

---

[638] UN Human Rights Committee, *Sergio Ruben Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981.
[639] UN Human Rights Committee, *Lilian Celiberti de Casariego v. Uruguay*, No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981.
[640] EGMR, *Issa and Others v. Turkey*, 31821/96, 16. November 2004, Rn. 71.
[641] *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 175.
[642] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011.
[643] Ebd., Rn. 33 ff.
[644] Ebd., Rn. 95.

Art. 1 EMRK primär auf das Staatsterritorium bezogen ist und extraterritoriale Handlungen nur ausnahmsweise umfasst sind.[645] Der Gerichtshof fasst anschließend die bislang in seiner Rechtsprechung anerkannten Ausnahmefälle für eine extraterritoriale Anwendung der Konvention ausführlich und umfassend zusammen. Dazu unterteilt er die Fälle in zwei Kategorien. So fasst er einerseits die Fallgruppen, die aufgrund einer personellen Kontrolle („*state agent authority and control*") eine extraterritoriale Geltung der Konvention begründen, in einer Kategorie zusammen.[646] Andererseits zählt er in der zweiten Kategorie die Fallgruppen auf, die wiederum aufgrund einer territorialen Kontrolle („*effective control over an area*") zur extraterritorialen Anwendbarkeit der EMRK führen.[647]

Anschließend wird die *espace-juridique*-Doktrin als allgemeines Prinzip vorgebracht. Im Gegensatz zu seiner strikten Position im *Banković*-Urteil stellt der Gerichtshof jedoch an dieser Stelle nun fest, dass Jurisdiktion im Sinne des Art. 1 EMRK auch außerhalb des europäischen Konventionsrechtsraums bestehen könne.[648] Damit rückt der EGMR nun eindeutig von der strikten *espace-juridique*-Doktrin aus *Banković* ab, ohne jedoch die Doktrin als solche ausdrücklich aufzugeben.[649] Auch hinsichtlich des Anwendungsumfangs der Konvention in Fällen der extraterritorialen Jurisdiktion revidiert der EGMR seinen strengen Alles-oder-Nichts-Ansatz aus *Banković*. So können die Konventionsrechte in extraterritorialen Fällen proportional zum Maß der Kontrolle durch den Staat entsprechend der Einzelfallumstände teilweise angewendet werden.[650]

Mit dem Urteil im Fall *Al-Skeini and Others v. The United Kingdom* ist es dem Gerichtshof somit durchaus gelungen, seine uneinheitliche Rechtsprechung und insbesondere durch *Banković* verursachte Unklarheiten hinsichtlich der extraterritorialen Anwendbarkeit der EMRK weitgehend zu beseitigen.[651] Leider vermeidet der Gerichtshof dennoch, ausdrücklich und in aller Klarheit alle kritikwürdigen Ansätze im *Banković*-Urteil abzulehnen. Vielmehr versucht er die gesamte bisherige Rechtsprechung – inklusive *Banković* – als ein homogenes Spruchpraxis-Bild zusammenzufügen, obwohl der Gerichtshof durchaus indirekt *Banković* in vielen Aspekten revidiert und korrigiert hat.[652] Der EGMR hält jedoch weiterhin an die Regel-Ausnahme-Formel aus *Banković* fest. Die umfassende Aufzählung der Fallgruppen für eine exzeptionelle extraterritoriale Anwendung der Konvention sorgt jedoch für Kohärenz und gibt als Fallkatalog einen klaren Leitfaden über die vom EGMR

---

[645] Ebd., Rn. 131 f.

[646] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 133 ff.

[647] Ebd., Rn. 138 ff. Die in dieser Zusammenstellung aufgelisteten Fälle sind im folgenden Unterabschnitt im Detail dargestellt.

[648] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 141 f.

[649] *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 129.

[650] Siehe dazu 3. Abschnitt, Unterabschnitt A. I. 3. b.

[651] *Jankowska-Gilberg*, Das Al-Skeini-Urteil des Europäischen Gerichtshofs für Menschenrechte, S. 73.

[652] Milanovic argumentiert gleichermaßen: *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 127.

bislang anerkannten Anwendungsfälle extraterritorialer Jurisdiktion. Als eine wichtige Leitentscheidung wurde der Fall *Al-Skeini* insofern auch in vielen folgenden einschlägigen Urteilen des EGMR zitiert.[653]

c. Zwischenergebnis

Die Jurisdiktionsklauseln in Art. 2 Abs. 1 IPbpR und Art. 8 EMRK unterscheiden sich im Wortlaut. Daneben ist aber auch eine unterschiedliche Sichtweise der beiden Spruchkörper zur allgemeinen Frage über die extraterritoriale Anwendbarkeit der Menschenrechtspakte erkennbar. Obwohl der Wortlaut der Jurisdiktionsklausel im IPbpR durchaus Raum für Diskussionen lässt und tatsächlich bis heute unterschiedliche Sichtweisen über die Auslegung dieser Vorschrift herrschen, hat der MRA von Beginn an eine offene Haltung zu dieser Fragestellung eingenommen.[654] Der Ausschuss hat seit jeher eine extraterritoriale Anwendbarkeit des Paktes in aller Klarheit befürwortet und ist seiner Spruchpraxis treu geblieben. Hingegen hat sich der EGMR in seiner Jurisprudenz deutlich schwerer getan, die extraterritoriale Anwendbarkeit der EMRK aus Art. 1 EMRK abzuleiten.[655] Obwohl gerade der Wortlaut dieser Jurisdiktionsklausel einen offenen Jurisdiktionsbegriff ohne weiteres zulässt und im Gegensatz zum IPbpR auch nicht zweideutig formuliert ist. Der EGMR hat dennoch einen restriktiven Standpunkt eingenommen, der insbesondere in der Entscheidung *Banković* erkennbar wurde. Die anschließende Rechtsprechung des EGMR hat indes allmählich den Raum für eine extraterritoriale Anwendbarkeit der Konvention geöffnet, indem Ausnahmen zur extraterritorialen Unanwendbarkeit der Konvention konstruiert wurden.

Trotz dieser unterschiedlichen Grundhaltungen der beiden Spruchkörper und ihren divergenten Begründungsansätzen zur extraterritorialen Anwendbarkeit der Menschenrechtspakte, lassen sich die bisher von ihnen entschiedenen Anwendungsfälle gemeinsam kategorisieren. Die bisher vom MRA und EGMR entschiedenen Fallgruppen zur extraterritorialen Geltung der Paktbestimmungen werden nachfolgend dargestellt.

---

[653] So etwa in EGMR, *Hirsi Jamaa and others v. Italy* [GC], Rs. 27765/09, 23. February 2012, Rep. 2012; EGMR, *Catan and Others v. Moldova and Russia* [GC], Rs. 43370/04, 18454/06, 8252/05, 19. Oktober 2012, Rep. 2012; EGMR, *Hassan v. The United Kingdom* [GC], Rs. 29750/09, 16. September 2014, Rep. 2014; *Jaloud v. The Netherlands* [GC], Rs. 47708/08, 20. November 2014, Rep. 2014.

[654] *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 111.

[655] *Shany,* Taking Universality Seriously, S. 51.

2. *Voraussetzung der extraterritorialen Anwendbarkeit des IPbpR und der EMRK: Die extraterritoriale Jurisdiktionsausübung*

„Jurisdiktion" beschreibt – wie oben dargestellt – die zwischen einem Staat und einem Individuum bestehende Beziehung, die durch die Gewalt des Staates über konkrete Personen oder über bestimmte Territorien, auf denen sich diese Personen befinden, begründet wird. Diese Staatsgewalt äußert sich wiederum insbesondere durch staatliche Kontrolle. In der bislang zusammengestellten Spruchpraxis hat sich soweit gezeigt, dass der MRA und der EGMR im Rahmen extraterritorialer Sachverhalte auch auf das Bestehen von Kontrolle durch den Vertragsstaat abstellen. Allerdings unterscheiden sich die Kontrollbegriffe der beiden Spruchkörper.

So übt ein Staat außerhalb seines eigenen Territoriums Jurisdiktion im Sinne der Art. 2 Abs. 1 IPbpR, wenn er über ein bestimmtes Gebiet oder über konkrete Individuen faktische Kontrolle verfügt. Die sogenannte „effektive Kontrolle" im weiteren Sinne ist somit für die extraterritoriale Anwendbarkeit des IPbpR ein Schlüsselmerkmal. So stellt der Menschenrechtsausschuss im *General Comment* 31 in diesem Sinne fest:

> „States Parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. […], the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals […], who may find themselves in the territory or subject to the jurisdiction of the State Party."[656]

Mit der Formulierung „*power or effective control*" nennt der Ausschuss das Kriterium dafür, wann eine Person unter der Jurisdiktion des Staates steht. So muss sich die Person unter der effektiven Kontrolle des Staates befinden. Diese Kontrolle kann rechtlich oder faktisch sein.[657]

Zwar geht der EGMR grundsätzlich davon aus, dass Jurisdiktion nach Art. 1 EMRK primär auf dem Staatsgebiet der Vertragsstaaten ausgeübt wird und sich nur ausnahmsweise auf extraterritoriale Fälle erstreckt. Aber auch im Rahmen dieser extraterritorialen Ausnahmefälle stellt der Gerichtshof auf die Kontrolle des Staates ab. So ist ein Vertragsstaat an die EMRK gebunden, wenn er Kontrolle und Macht

---

[656] UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 10.

[657] Siehe dazu bereits oben 3. Abschnitt, Unterabschnitt A. I. 1. a. aa.

über Individuen („*state agent authority and control*“) oder effektive Kontrolle über ein Territorium („*effective control over an area*“) ausübt.[658]

Beide Spruchkörper haben indes keine umfassende Definition der Begriffe „*effective control*“ sowie „*state authority and control*“ in diesem Zusammenhang entwickelt. Vielmehr gehen bisher der Menschenrechtsausschuss und insbesondere der EGMR kasuistisch vor. So hat der MRA in den bisher einschlägigen *Views* und im Kontext einschlägiger *Concluding Observations* anhand der Umstände der konkreten Sachlage über das Bestehen der Kontrolle entschieden.[659] Auch im zitierten *General Comment* 31 ist keine allgemeine und detaillierte Definition von „*power or effective control*“ vorhanden. Vielmehr zählt der Ausschuss hier ebenfalls zur Spezifizierung des Kontrollbegriffs einzelne Fallbeispiele auf.[660] In der umfangreichen Spruchpraxis des EGMR ist die kasuistische Vorgehensweise sogar noch deutlicher zu erkennen,[661] wobei der Gerichthof insgesamt wenig kohärent vorgegangen ist.[662]

Die bisher entwickelten Kriterien für das Vorliegen von „*state authority and control*“ in extraterritorialen Fällen hat der EGMR erstmals in der Entscheidung *Al-Skeini* systematisiert.[663] Aber auch hier entwickeln die Straßburger Richter keineswegs eine allgemeine Formel für den Kontrollbegriff, sondern fügen die bislang anerkannten Fallgruppen von effektiver Kontrolle und extraterritorialer Anwendbarkeit der EMRK in einem systematischen Katalog zusammen.

Es ist zudem irrelevant, ob die Jurisdiktionsausübung legal oder rechtswidrig ausgeübt wird.[664] So spielt es für die Feststellung der extraterritorialen Jurisdiktion keine Rolle, ob ein Staat rechtlich zur Ausübung der Kontrolle auf fremden Staatsgebiet – etwa aufgrund bilateraler Abkommen oder in Form von Interventionen auf Einladung – befugt ist oder nicht.[665] Anderenfalls käme man zu dem absurden Ergebnis, dass ein rechtwidrig agierender Staat per se nicht an seine Menschenrechtsverpflichtungen aus den Pakten gebunden wäre.

---

[658] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 131 ff. Vgl. auch *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 153 f.

[659] So auch *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 89.

[660] UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 10.

[661] *Szydlo,* Extra-Territorial Application of the European Convention on Human Rights after Al-Skeini and Al-Jedda, S. 283.

[662] Dazu ausführlich 3. Abschnitt, Unterabschnitt A. I. 1. b. aa.–cc.

[663] Siehe oben 3. Abschnitt, Unterabschnitt A. I. 1. b. cc.

[664] *Wilde,* State Obligations Extraterritorially, S. 508 und 513f; *Milanovic,* Extraterritorial Application of Human Rights Treaties, S. 27.

[665] Dies hat der Menschenrechtsausschuss im *General Comment* 31 eindeutig festgestellt: „This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, *regardless of the circumstances in which such power or effective control was obtained*“, UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 10 [Hervorh. d. Verf.].

In Sinne dieser kasuistischen Praxis werden im Folgenden die bislang von beiden Spruchkörpern anerkannten Fallgruppen dargestellt. Dabei erfolgt eine – der Jurisprudenz beider Spruchkörper entsprechenden – Unterteilung zwischen Fällen der territorialen Kontrolle sowie Fällen, in denen personelle Kontrolle ausgeübt wird.

a. Jurisdiktionsausübung aufgrund territorialer Kontrolle

Als klassischer Fall der effektiven territorialen Kontrolle außerhalb des eigenen Staatsgebiets ist die militärische Besetzung eines Staates als extraterritoriale Jurisdiktionsausübung sowohl vom Menschenrechtsausschuss sowie vom EGMR unbestritten anerkannt.

Insbesondere im Rahmen der Staatenberichtsverfahren von Israel hebt der Menschenrechtsausschuss regelmäßig in seinen *Concluding Observations* hervor, dass die Paktgarantien auch in den besetzten Gebieten Palästinas umgesetzt werden müssen.[666]

Im Urteil *Loizidou* als Leitentscheidung des EGMR zur extraterritorialen Anwendung der EMRK in militärischen Besatzungssituationen stellte der Gerichtshof fest, dass die Konventionspflichten der Staaten auch dann bestehen, wenn diese infolge von militärischen Operationen effektive Kontrolle über ein fremdes Staatsgebiet ausüben.[667] Mit Verweis auf diese Leitentscheidung hebt der EGMR in *Al-Skeini* hervor, dass aufgrund der faktischen Kontrolle, ausgeübt durch eigene militärische Streitkräfte oder durch die nachgeordnete Lokalverwaltung, die Staaten zur Zusicherung der Konventionsrechte verpflichtet seien.[668] Des Weiteren benennt der Gerichtshof hier Kriterien, wonach sich das Bestehen effektiver Gebietskontrolle beurteilen lässt. Maßgeblich sei demnach die Stärke der militärischen Präsenz im besetzten Gebiet.[669] Außerdem kann das Maß der militärischen, wirtschaftlichen und politischen Unterstützung für die untergeordnete Lokaladministration hinsichtlich der Jurisdiktionsausübung des unterstützenden Staates relevant sein.[670]

Über militärische Besatzungssituationen eines Einzelstaates hinaus kann auch die Beteiligung staatlicher Streitkräfte im Rahmen von friedenssichernden Einsätzen

---

[666] UN Human Rights Committee, Concluding observations: Israel, CCPR/C/79/Add. 93, 18. August 1998, Rn. 10; Concluding observations: Israel, CCPR/CO/78/ISR, 21. August 2003, Rn. 11; Concluding observations: Israel, CCPR/C/ISR/CO/3, 3. September 2010, Rn. 5; Concluding observations: Israel, CCPR/C/ISR/CO/4, 21. November 2014, Rn. 5. Auch der IGH hat dies bestätigt, siehe dazu bereits oben 3. Abschnitt, Unterabschnitt A. I. 1. a. bb. Vgl. außerdem UN Human Rights Committee, Concluding observations: Iraq, A/46/40 (Rn. 618–656), 10. Oktober 1991, Rn. 652 und Concluding observations: USA, CCPR/C/USA/CO/3, 15. September 2006, Rn. 10.

[667] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Preliminary Objections), 23. März 1995, Serie A 310, Rn. 62. Außerdem *Cyprus v. Turkey* [GC], Rs. 25781/94, 10. Mai 2001, Rep. 2001-IV.

[668] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 138.

[669] Ebd., Rn. 139.

[670] Ebd., mit Verweis auf EGMR *Ilașcu and Others v. Moldova and Russia* [GC], Rs. 48787/99, 8. Juli 2004, Rep. 2004-VII. Kritisch dazu *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 157 f.

internationaler Organisationen in Drittstaaten die territoriale Kontrolle und infolgedessen die Jurisdiktionsausübung des beteiligten Staates auslösen. Voraussetzung hierfür ist indes, dass verursachte Menschenrechtsverletzungen dem beteiligten Staat sowie seinen agierenden Streitkräften und nicht der federführenden internationalen Organisation zuzurechnen sind. Diese Möglichkeit der territorialen Kontrolle geht aus *General Comment* 31 des Menschenrechtsausschusses ausdrücklich hervor[671] und wird zudem in einer Reihe von *Concluding Observations* genannt.[672] Die Leitentscheidung des EGMR zu diesem Themenbereich ist die Entscheidung *Behrami and Behrami v. France and Saramati v. France, Germany and Norway.*[673]

b. Jurisdiktionsausübung aufgrund personeller Kontrolle

Übt ein Staat über einzelne Individuen außerhalb seines Staatsgebiets Kontrolle aus, ohne dabei über territoriale Kontrolle auf dem fremden Staatsgebiet zu verfügen, so liegt ein Fall der personellen Jurisdiktion vor. Anknüpfungspunkt dieser Fallgruppen ist nicht etwa ein territorialer Bezug, sondern vielmehr der „*jurisdictional link*" zwischen dem Staat und den betroffenen Individuen.

aa. Jurisdiktionsausübung in diplomatischen Vertretungen und an Bord von Schiffen und Flugzeugen

Diplomatische Organe, die im Ausland staatliche Hoheitsgewalt in konsularischen und diplomatischen Vertretungen ausüben, sind an die Menschenrechtsverpflichtungen aus den Pakten gebunden. Die extraterritoriale Verpflichtung der Staaten hinsichtlich dieser Fallgruppe wird vom EGMR und vom MRA unbestritten angenommen.[674] Der MRA befasste sich in einer Reihe von Fällen gegen Uruguay mit der Frage, ob die Verweigerung diplomatischer Staatsvertreter, einen Pass auszustellen oder zu erneuern, einen Verstoß gegen die Menschenrechtsverpflichtungen aus dem IPbpR darstellt.[675] Hinsichtlich der Anwendbarkeit des Paktes im Rahmen dieses Auslands-Sachverhalts stellte der Ausschuss folgendes fest:

---

[671] UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 10.

[672] UN Human Rights Committee, Concluding observations: Belgium, CCPR/CO/81/BEL, 12. August 2004, Rn. 6; Concluding observations: Netherlands, CCPR/CO/72/NET, 27. August 2001, Rn. 8. Siehe dazu auch *Joseph/Castan,* The International Covenant on Civil and Political Rights, Rn. 4.16 m.w.N.

[673] EGMR, *Behrami and Behrami v. France and Saramati v. France, Germany and Norway* [GC], Rs. 71412/01, 78166/01, 2. Mai 2007. Zentrale Frage dieser Entscheidung war, ob die Konventionsstaaten für konventionswidrige Handlungen und Unterlassungen ihrer Truppen im Kosovo verantwortlich sind, die sie den multinationalen Militäreinsätzen KFOR (Kosovo Force) und UNMIK (United Nations Mission in Kosovo) zur Verfügung gestellt haben.

[674] *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 156.

[675] UN Human Rights Committee, *Sophie Vidal Martins v. Uruguay*, No. 057/1979, CCPR/C/15/D/57/1979, 23. März 1982; *Samuel Lichtensztejn v. Uruguay*, No. 77/1980,

„The issue of a passport to a Uruguayan citizen is clearly a matter within the jurisdiction of the Uruguayan authorities and he is ‚subject to the jurisdiction' of Uruguay for that purpose. […] therefore, article 2 (1) of the Covenant could not be interpreted as limiting the obligations of Uruguay under article 12 (2) to citizens within its own territory."[676]

Die EKMR hat wiederum bereits in den 60er- und 70er-Jahren die extraterritoriale Verpflichtung von staatlichen Organen in konsularischen und diplomatischen Vertretungen im Grundsatz festgestellt.[677] Der EGMR hat diese Feststellung wiederum in seiner Jurisprudenz bestätigt.[678]

Auch auf Schiffen und in Flugzeugen kann ein Staat nach Ansicht des EGMR Jurisdiktion über Individuen, die sich an Bord von Schiffen und Flugzeugen befinden, ausüben.[679] Diese Jurisdiktionsausübung kann entweder aufgrund der Flaggenhoheit begründeten *de jure*-Kontrolle über die Besatzung und Personen, die sich an Bord aufhalten, bestehen. So entschied der EGMR etwa im Fall *Hirsi Jamaa and Others v. Italy*, in dem Asylsuchende, die auf hoher See in Seenot geraten sind, von der italienischen Küstenwache mit Schiffen nach Libyen zurückgeführt wurden. Hier spielte auch die Tatsache, dass es sich um ein Schiff der italienischen Küstenwache handelte, eine wichtige Rolle für die Begründung der Kontrolle. Die Beschwerdeführer befanden sich hier vom Zeitpunkt des Betretens des italienischen Schiffes bis zur Übergabe an die lybischen Organe unter der ununterbrochenen und ausschließlichen *de jure*- und *de facto*- Jurisdiktion Italiens, so die Argumentation des EGMR.[680]

In der Entscheidung *Medvedyev and Others v. France* stellen die Straßburger Richter indes klar, dass ein Staat auch aufgrund der unmittelbaren und ausschließlichen *de facto*-Kontrolle an Bord eines Schiffes, das offiziell unter fremder Flagge segelt, über die Besatzung Jurisdiktion ausüben kann.[681] Richtigerweise stellt der EGMR für diese Fallkategorie fest, dass nicht allein die Kontrolle über den Aufenthaltsort der

CCPR/C/18/D/77/1980, 31. März 1983; *Mabel Pereira Montero v. Uruguay,* No. 106/1981, CCPR/C/18/D/106/1981, 31. März 1983; *Carlos Varela Nunez v. Uruguay,* No. 108/1981, CCPR/C/19/D/108/1981, 22. Juli 1983.

676 UN Human Rights Committee, *Samuel Lichtensztejn v. Uruguay*, No. 77/1980, CCPR/C/18/D/77/1980, 31. März 1983, Rn. 6.1. Siehe außerdem *Shany,* Taking Universality Seriously, S. 52–53.

677 EKMR, *X. v. The Federal Republic of Germany,* Rs. 1611/62, 25. September 1965, Yearbook 8, S. 158
(S. 168); EKMR, *X. v. the United Kingdom*, Rs. 7547/76, 15. Dezember 1977, D.R. 12, S. 73 (S. 74).

678 EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 134.

679 Ebd., Rn. 136; EGMR, *Hirsi Jamaa and Others v. Italy* [GC], Rs. 27765/09, 23. February 2012, Rep. 2012, Rn. 75.

680 Ebd., Rn. 81.

681 EGMR, *Medvedyev and Others v. France*, Rs. 3394/03, 29. März 2010, Rep. 2010, Rn. 66. In diesem Fall übte Frankreich faktische Kontrolle über ein unter der Flagge Kambodschas fahrendes Schiff aus.

Personen – d.h. in Flugzeugen und Schiffen – die Jurisdiktion der Staatsorgane begründe. Vielmehr sei in diesen Fällen die tatsächliche Ausübung physischer Gewalt und Kontrolle über die Personen entscheidend.[682]

bb. Unmittelbare Gewalt und Kontrolle über einzelne Individuen

Die Ausübung von unmittelbarer physischer Gewalt und Kontrolle gegenüber Individuen durch einen Staat außerhalb seines Hoheitsgebiets begründet die Jurisdiktion desselben über die betroffenen Individuen.

(1) Festnahme und Inhaftierung von Individuen

Die Festnahme und Inhaftierung von Individuen auf fremden Staatsgebiet stellt einen anerkannten Fall der extraterritorialen Jurisdiktion dar, die die Bindung der agierenden staatlichen Organe an die Menschenrechtsverträge begründet.[683] In solchen Fällen gezielter hoheitlicher Operationen außerhalb des Staatsgebiets üben die Organe eines Vertragsstaates nämlich Hoheitsgewalt und Kontrolle über konkrete Personen aus. Mit seinen *Views* in den Fällen *Lopez Burgos v. Uruguay* und *Celiberti de Casariego v. Uruguay*, die gerade die Festnahme und Entführung uruguayischer Oppositioneller aus Argentinien betrafen, hat der Menschenrechtsauschuss damit schon sehr früh diesen Standpunkt in aller Deutlichkeit eingenommen.[684]

Der EGMR entschied im Fall *Öcalan v. Turkey*, dass die Türkei Jurisdiktion über den PKK-Führer Abdullah Öcalan auf kenianischem Territorium ausübte, nachdem derselbe von kenianischen Organen auf dem Flughafen in Nairobi an die türkischen Organe übergeben wurde und sich somit in türkischem Gewahrsam befand.[685] Die Jurisdiktion des Vereinigten Königreichs im Fall *Al-Saadoon and Mufdhi v. The United Kingdom*, der die Inhaftierung zweier Iraker in britisch geführten Gefängnissen im Irak zum Gegenstand hatte, begründete der EGMR mit der ausschließlichen und umfassenden Kontrolle Großbritanniens über jenes Gefängnis und den dort inhaftierten Individuen.[686] Die Tatsache, dass sich das Gefängnis außerhalb britischen Territoriums befand, stand der Jurisdiktionsausübung im Sinne des Art. 2 EMRK nach Ansicht des EGMR nicht entgegen. Auch in dieser

[682] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 136.
[683] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 136.
[684] 3. Abschnitt, Unterabschnitt A. I. 1. a. aa.
[685] EGMR, *Öcalan v. Turkey* [GC], Rs. 46221/99, 12. Mai 2005, Rep. 2005-IV, Rn. 91. Hier stellt der Gerichtshof erstmals fest, dass ein Staat auch punktuell extraterritoriale Jurisdiktion über eine Person ausüben kann. Siehe dazu bereits 3. Abschnitt, Unterabschnitt A. I. 1. b. cc. Dieser Standpunkt des EGMR geht ebenso aus EGMR, *Issa and Others v. Turkey,* 31821/96, 16. November 2004 hervor.
[686] EGMR, *Al-Saadoon and Mufdhi v. the United Kingdom*, Rs. 61498/08, 30. Juni 2009, Rn. 88. Siehe außerdem EGMR, *Hassan v. The United Kingdom* [GC], Rs. 29750/09, 16. September 2014, Rep. 2014, Rn. 76.

Fallgruppe ist die tatsächliche Ausübung physischer Gewalt und Kontrolle über die Personen für die Jurisdiktionsausübung entscheidend.[687]

(2) Gezielte Tötungen

Ob ein Staat durch gezielte Tötungshandlungen auf fremdem Staatsgebiet Jurisdiktion über die betroffenen Individuen ausübt, ohne dabei in jeglicher Weise zugleich Kontrolle über dieses Territorium zu haben, ist vom EGMR nicht kohärent beantwortet worden.

Hinsichtlich der Bombardierungen und Tötung von Zivilisten im Fall *Banković* hat der Gerichtshof aufgrund der fehlenden effektiven territorialen Kontrolle der beteiligten NATO-Staaten eine Jurisdiktion abgelehnt, ohne zudem ausdrücklich der Frage nachzugehen, ob allein die Tötungshandlung als solche den „*jurisdictional link*" zwischen den Staaten und den Individuen begründet haben könnte.[688] Erst in späteren Urteilen hat der Gerichtshof diese Möglichkeit der Jurisdiktionsausübung überhaupt in Erwägung gezogen. So wurde hinsichtlich der Tötung irakischer Schafshirten durch einen Militäreinsatz der Türkei im Nordirak in der Entscheidung *Issa and Others v. Turkey* erstmals vom Gerichtshof die Alternative untersucht, ob sich die betroffenen Personen unter der unmittelbaren Gewalt und Kontrolle der Türkei befanden.[689] In der Entscheidung *Al-Skeini* räumt der EGMR interessanterweise ausdrücklich ein, dass sich die Personen im Fall *Issa* – sofern die Festnahme und Hinrichtung durch türkische Soldaten bewiesen worden wäre – durchaus unter türkischer Jurisdiktion befunden hätten.[690]

Im Fall *Pad and Others v. Turkey* wurden iranische Staatsangehörige im Grenzgebiet zwischen der Türkei und Iran von einem türkischen Helikopter aus erschossen, da die Türkei diese für terrorverdächtig hielt. Ob sich die Personen zum Todeszeitpunkt auf türkischem oder iranischem Staatsgebiet befanden, war unklar. Die Türkei hat aber nicht bestritten, dass die Schüsse von einem türkischen Helikopter ausgingen:

> „However, in the instant case, it was not disputed by the parties that the victims of the alleged events came within the jurisdiction of Turkey. While the applicants attached great importance to the prior establishment of the exercise by Turkey of extraterritorial jurisdiction with a view to proving their allegations on the merits, the Court considers that it is not required to

[687] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 136.

[688] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 74 ff.

[689] EGMR, *Issa and Others v. Turkey*, 31821/96, 16. November 2004, Rn. 74 f. Siehe zudem *Jankowska-Gilberg*, Das Al-Skeini-Urteil des Europäischen Gerichtshofs für Menschenrechte, S. 66.

[690] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 136. Siehe außerdem auch EGMR, *Jaloud v. The Netherlands* [GC], Rs. 47708/08, 20. November 2014, Rep. 2014.

> determine the exact location of the impugned events, given that the Government had already admitted that the fire discharged from the helicopters had caused the killing of the applicants' relatives, who had been suspected of being terrorists."[691]

Der Gerichtshof bejaht in diesem Fall die Jurisdiktionsausübung der Türkei. In diesem Urteil stützt sich der EGMR darauf, dass die Türkei die Jurisdiktion nicht in Frage stellte. Interessant ist dennoch, dass hier der EGMR die Jurisdiktion nicht in Frage stellte, obwohl es sich doch um eine gezielte Tötung handelte und die Türkei keinerlei öffentliche territoriale Gewalt über Iran ausübte. Diese Entscheidung steht insofern – bei durchaus ähnlicher Sachverhaltslage – in einem Gegensatz zur *Banković*-Rechtsprechung und dem vom EGMR vertretenen „*cause-and-effect*" Ansatz.[692]

Auch für die Tötungshandlungen im Fall *Al-Skeini*[693] hat der Gerichtshof aufgrund personeller Kontrolle die Jurisdiktionsausübung des Vereinigten Königreiches bejaht. Dabei kam in diesem Fall der besondere Umstand hinzu, dass Großbritannien im Südostirak – dem Gebiet der Tötungshandlungen – für die Aufrechterhaltung der Sicherheit verantwortlich war und damit mitunter öffentliche Gewalt ausübte:

> „[The] United Kingdom (together with the United States of America) assumed in Iraq the exercise of some of the public powers normally to be exercised by a sovereign government. In particular, the United Kingdom assumed authority and responsibility for the maintenance of security in south-east Iraq. In these exceptional circumstances, the Court considers that the United Kingdom, through its soldiers engaged in security operations in Basra during the period in question, exercised authority and control over individuals killed in the course of such security operations, so as to establish a jurisdictional link between the deceased and the United Kingdom for the purposes of Article 1 of the Convention."[694]

Damit stellt hier der Gerichtshof nicht allein auf die personelle Kontrolle ab, sondern zieht zudem die Ausübung öffentlicher Gewalt als zusätzliches Kriterium heran. Dabei stellt sich die Frage, ob der Gerichtshof dieses Kriterium nun generell als Voraussetzung für eine Jurisdiktionsausübung in Fällen von gezielten

---

[691] EGMR, *Pad and Others v. Turkey*, Rs. 60167/00, 28. Juni 2007, Rn. 54.

[692] *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 124. Siehe in diesem Zusammenhang auch EGMR, *Isaak v. Turkey,* Rs. 44587/98, 24. Juni 2008. In diesem Fall wurde ein Zypriot unter Beteiligung von türkisch-zypriotischen Polizisten in einer UN-Pufferzone – und somit außerhalb des territorialen Kontrollgebiets der Türkei – zu Tode geprügelt. Der EGMR bejahte die Jurisdiktionsausübung der Türkei aufgrund personeller Kontrolle.

[693] Zum Sachverhalt dieser Entscheidung siehe bereits 3. Abschnitt, Unterabschnitt A. I. 1. b. cc.

[694] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 149. Siehe außerdem *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 130.

Tötungshandlungen ansieht oder aber dies nur in diesem konkreten Fall als zusätzliches Argument heranzieht.[695] Gegen letzteres spricht zwar, dass dies mit der bis heute vertretenen „*cause-and-effect*"-Rechtsprechung des EGMR nicht zu vereinbaren wäre. Auf der anderen Seite stellt der Gerichtshof selbst im *Al-Skeini*-Urteil nur wenige Absätze vorher fest, dass eine personelle Kontrolle etwa in Fällen von Festnahmen außerhalb des Staatsgebiets anzunehmen ist, ohne dass es auf die Ausübung öffentlicher Gewalt ankäme. Entscheidend sei allein, dass der Staat physische Gewalt und Kontrolle über die Personen ausübe.[696] Angesichts dessen erscheint es widersprüchlich, für gezielte Tötungen zusätzlich zwingende Voraussetzungen festzulegen, während diese Voraussetzungen für eine Festnahme allein nicht erforderlich wären. Dies gilt insbesondere angesichts der Tatsache, dass die staatliche Entscheidung über die Ausführung einer Exekution Ausdruck höchster Hoheitsgewalt und staatlichen Zwangs ist.[697]

In der Spruchpraxis des Menschenrechtsausschusses ist bislang keine ausdrückliche Stellungnahme zum konkreten Fall der gezielten Tötungshandlungen zu finden. Allerdings hat sich der Ausschuss eben auch nicht gegen eine personelle Kontrolle durch gezielte Tötungshandlungen positioniert. Vielmehr sprechen die Leitentscheidungen *Lopez Burgos v. Uruguay* und *Celiberti de Casariego v. Uruguay* dafür, dass der Ausschuss für die Feststellung der Jurisdiktion durchaus auch auf gezielte Einzelakte abstellt, ohne dabei zusätzliche Kriterien heranzuziehen.[698] Hier ist nicht ersichtlich, warum der Ausschuss für extraterritoriale Tötungshandlungen strengere Maßstäbe ansetzen sollte. Dabei sei an dieser Stelle wiederum auf die weite Auslegung des Art. 2 Abs. 1 IPbpR durch den Ausschuss und seine grundsätzlich offene Haltung hinsichtlich der extraterritorialen Anwendbarkeit des Paktes verwiesen.[699]

3. Rechtsfolgen: Die Reichweite der extraterritorialen Verpflichtungen

Konventionsstaaten sind auch außerhalb ihres Territoriums an ihren Verpflichtungen aus den Menschenrechtspakten gebunden, wenn sie extraterritoriale Jurisdiktion ausüben. Im Rahmen der Jurisdiktionsausübung gibt es keine Abstufungen, denn entweder übt ein Staat bei Vorliegen aller Voraussetzungen Jurisdiktion aus oder im umgekehrten Fall eben nicht.[700] Dabei macht es auch keinen qualitativen Unterschied, ob die Jurisdiktion innerhalb der eigenen Staatsgrenzen ausgeübt wird oder aber extraterritorial. Davon zu unterscheiden ist indes die Frage nach dem Umfang der infolge von extraterritorialer Jurisdiktionsausübung bestehenden

[695] Milanovic leitet z.B. daraus ab, dass der EGMR anders entschieden hätte, wenn keine Ausübung öffentlicher Gewalt gegeben wäre. *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 130.
[696] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 136.
[697] So auch *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 162; *Jankowska-Gilberg,* Das Al-Skeini-Urteil des Europäischen Gerichtshofs für Menschenrechte, S. 69 f. mit weiteren Argumenten.
[698] *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 161.
[699] Sieh oben 3. Abschnitt, Unterabschnitt A. I. 1. a. aa.
[700] *Besson,* The Extraterritoriality of the European Convention on Human Rights, S. 878.

Menschenrechtsverpflichtungen im Ausland. Dies betrifft die Rechtsfolgenseite der extraterritorialen Anwendbarkeit der Menschenrechtspakte. Bislang wurde nämlich festgestellt, dass Handlungen eines Staates im Ausland seine extraterritoriale Verpflichtung aus den Menschenrechtspakten begründen kann. Offen ist hingegen noch die Frage nach der Reichweite der extraterritorialen Menschenrechtsverpflichtung des Staates. In diesem Sinne wird nachfolgend eben diese Frage untersucht.

Im Raum steht einerseits die Verpflichtung der Staaten, vollumfänglich alle Pflichten aus den Menschenrechtsverträgen gegenüber den Personen, die unter ihrer extraterritorialen Jurisdiktion stehen, umzusetzen. In diesem Fall wäre letztlich der Umfang der extraterritorialen Pflichten identisch mit den Verpflichtungen des Staates auf dem eigenen Staatsterritorium. Daneben kommt aber auch eine partielle – am Umfang der konkreten Kontrollausübung des Staates gemessenen – Umsetzung der Menschenrechte aus dem IPbpR und der EMRK in Betracht. Hierbei läge wiederum eine Reduzierung des staatlichen Pflichtmaßes im Vergleich zu den Menschenrechtsverpflichtungen im eignen Territorium vor. Naheliegend erscheint grundsätzlich die Annahme, dass mit Begründung von Jurisdiktion die Staaten vollumfänglich an ihren Verpflichtungen aus den Menschenrechtspakten gebunden sind, unabhängig davon, ob die Jurisdiktion innerhalb oder außerhalb der Staatsgrenzen ausgeübt wird. Denn es darf – im Sinne der Universalität der Menschenrechte – keinen Unterschied machen, ob ein Staat innerhalb oder außerhalb seiner Staatsgrenzen Jurisdiktion ausübt. Für diese These spricht auch der Wortlaut der Jurisdiktionsklauseln aus Art. 2 Abs. 1 IPbpR und Art. 1 EMRK. Denn die Jurisdiktionsklauseln besagen einzig, dass bei Vorliegen der Jurisdiktion die Staaten zum Schutz der kodifizierten Menschenrechte verpflichtet sind. Eine ausdrückliche Begrenzung ist nicht ausformuliert. Dennoch wird in bestimmten Fällen eine Begrenzung des Pflichtumfangs der Staaten diskutiert. Dabei wird in der Judikatur – insbesondere in der Spruchpraxis des EGMR – und von zahlreichen Stimmen in der Literatur zwischen der Jurisdiktionsausübung aufgrund umfassender Gebietskontrolle einerseits und der effektiven Personenkontrolle andererseits unterschieden.

a. Umfang der extraterritorialen Verpflichtungen in Fällen der effektiven Gebietskontrolle

Sowohl der MRA als auch der EGMR haben in ihrer Spruchpraxis anerkannt, dass in Fällen umfassender Gebietskontrolle eines Staates über ein fremdes Territorium eine vollumfängliche Geltung aller Bestimmungen und Verpflichtungen des extraterritorial agierenden Staates besteht. Der extraterritorial agierende Staat ist in diesem Fall gegenüber den Individuen im kontrollierten Gebiet an seine negativen Pflichten und ebenso an seine positiven Pflichten – wie etwa den Schutzpflichten – gebunden.[701] Richtigerweise wird in der Literatur in diesem Zusammenhang darauf

[701] *Besson,* The Extraterritoriality of the European Convention on Human Rights, S. 879. Besson stellt hier richtigerweise heraus, dass die extraterritoriale Umsetzung positiver Pflichten eine umfassende effektive Kontrolle bedarf.

hingewiesen, dass eine extraterritoriale Umsetzung von positiven Menschenrechtspflichten nur auf Basis einer umfassenden effektiven Kontrolle möglich sei. Tatsächlich können bestimmte Schutz- und Leistungspflichten nur dann extraterritorial umgesetzt werden, wenn etwa eine effektive Kontrolle der lokalen Verwaltungs- und Institutionsstrukturen gegeben ist.[702]

Der Menschenrechtsausschuss hat in seinen *Concluding Observations* zum israelischen Staatenbericht von 2010 festgestellt, dass Israel aufgrund seiner umfassenden Gebietskontrolle palästinensischer Territorien zur vollumgänglichen Gewährung aller Menschenrechte aus dem IPbpR verpflichtet ist:

> „The State party should ensure the full application of the Covenant in Israel as well as in the occupied territories, including the West Bank, East Jerusalem, the Gaza Strip and the occupied Syrian Golan Heights. In accordance with the Committee's general comment No. 31, the State party should ensure that all persons under its jurisdiction and effective control are afforded the full enjoyment of the rights enshrined in the Covenant."[703]

Diese Aussage des MRA erfolgte zwar speziell für den israelischen Staatenbericht. Allerdings kann durchaus davon ausgegangen werden, dass diese auf Israel bezogene Feststellung Ausdruck einer grundsätzlichen Sichtweise des Ausschusses ist. Die jurisdiktionsausübenden Staaten, die umfassende Gebietskontrolle über fremde Territorien ausüben, sind mithin nach Auffassung des MRA zur umfassenden Achtung und Gewährleistung der im IPbpR verbürgten Menschenrechte gegenüber den Individuen auf dem kontrollierten Gebiet verpflichtet.

Im Urteil *Cyprus v. Turkey* hat der EGMR wiederum festgestellt, dass die „TRNC"[704] umfassende effektive Kontrolle über Nordzypern ausübe und die Türkei für die Akte und Handlungen der „TRNC" auf dem zypriotischen Gebiet verantwortlich ist. Aufgrund dieser umfassenden Gebietskontrolle stellt der EGMR Folgendes fest:

> „Turkey's ‚jurisdiction' must be considered to extend to securing the entire range of substantive rights set out in the Convention and those additional Protocols which she has ratified, and that violations of those rights are imputable to Turkey".[705]

Somit sei die Türkei in diesem Fall vollumfänglich an ihre Verpflichtungen aus der Konvention und der Zusatzprotokolle gegenüber den Individuen in Nordzypern

[702] Dies wird insbesondere in Fällen der umfassenden Kontrolle eines fremden Territoriums anzunehmen sein.

[703] UN Human Rights Committee, *Concluding observations*: Israel, CCPR/C/ISR/CO/3, 3. September 2010, Rn. 5.

[704] Siehe Fn. 582.

[705] EGMR, *Cyprus v. Turkey* [GC], Rs. 25781/94, 10. Mai 2001, Rep. 2001-IV, Rn. 77.

verpflichtet und für jegliche Verletzungen der verankerten Menschenrechte im kontrollierten Gebiet grundsätzlich verantwortlich. Auch in der nachfolgenden Judikatur hat der EGMR an diesem Grundsatz festgehalten[706] und dies zudem in der Entscheidung *Al-Skeini and Others v. The United Kingdom* erneut herausgestellt[707].

Insofern besteht Einigkeit darüber, dass in Fällen umfassender effektiver Kontrolle über fremde Territorien die Staaten zur vollumfänglichen Achtung und Gewährung aller Menschenrechte verpflichtet sind. Dies ist überzeugend. In Fällen der umfassenden Gebietskontrolle ist nicht ersichtlich, warum die Staaten nur zu einem begrenzten Umfang verpflichtet sein sollten. Denn infolge dieser umfassenden Gebietskontrolle üben sie extraterritoriale Jurisdiktion auf diesen Gebieten aus, die wiederum zu einer umfassenden Verpflichtung der Staaten unter den Menschenrechtsbestimmungen führen muss. Die umfassende Jurisdiktionsausübung eines Staates im Ausland ist mit der Jurisdiktion innerhalb des eigenen Staates faktisch gleichzustellen. In diesem Sinne muss der Staat seine Menschenrechtsverpflichtungen unter dem IPbpR und der EMRK gegenüber den Individuen innerhalb des kontrollierten Gebietes in gleichem Umfang wie gegenüber den Individuen innerhalb seiner Staatsgrenzen umsetzen.[708]

b. Umfang der extraterritorialen Verpflichtungen in Fällen der effektiven Personenkontrolle

Problematisch ist indes, inwieweit die Verpflichtungen aus den Verträgen gelten, wenn ein Staat extraterritoriale Jurisdiktion ausübt, ohne dabei umfassende Kontrolle über fremde Territorien auszuüben. Hierbei geht es insbesondere um den Fall der extraterritorialen Jurisdiktionsausübung aufgrund der Kontrolle einzelner Individuen im Ausland.[709] Überwiegend wird in dieser Konstellation eine umfassende Verpflichtung der Staaten abgelehnt und stattdessen für eine partielle Verpflichtung der Staaten, die sich am Maß der konkreten Kontrollausübung orientiert, plädiert.

Der EGMR hat in seiner Judikatur die Frage nach der Reichweite der Verpflichtungen der Konventionsstaaten in Fällen der extraterritorialen Kontrolle über

[706] EGMR, *Salomou and Others v. Turkey,* Rs. 36832/97, 24. Juni 2008, Rn. 47; *Kallis and Androulla Panayi v. Turkey,* Rs. 45388/99, 27. Oktober 2009, Rn. 26.

[707] EGMR*, Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 138.

[708] Eine *umfassende* Gebietskontrolle liegt indes beispielsweise nicht vor, wenn der extraterritorial agierende Staat nur über einen lokal eng begrenzten Bereich des Territoriums – und dementsprechend nicht über erhebliche Teile des fremden Staatsgebiets – temporär effektive Kontrolle ausübt. Da hier die Ausübung effektiver Kontrolle nicht mehr mit der weitreichenden staatlichen Hoheitsgewalt des extraterritorial agierenden Staates auf seinem eigenen Territorium vergleichbar ist und auch der ausgedehnte Charakter der extraterritorialen Handlung nicht mehr vorliegt, wäre in diesem Fall auch die Begrenzung der Paktverpflichtungen auf die Menschenrechte, die in der konkreten lokalen Kontrollausübung relevant sind, vertretbar. Siehe dazu auch *Murray,* Practitioners' Guide to Human Rights Law in Armed Conflict, S. 66 und S. 73.

[709] Zu den Fallgruppen der effektiven personellen Kontrolle siehe oben 3. Abschnitt, Unterabschnitt A. I. 2. b.

einzelne Individuen nicht einheitlich beantwortet. Erstmals hat sich der Gerichtshof im Fall *Banković and Others v. Belgium and Others*[710] mit der Fragestellung befasst, ob Staaten proportional zum Umfang ihrer extraterritorialen Kontrolle in reduziertem Maße an ihre Konventionsverpflichtungen gebunden sind. Der Gerichtshof lehnte jedoch eine teilweise Anwendung der Konvention, gemessen am Maß der ausgeübten Jurisdiktion, ab. Vielmehr vertritt der Gerichtshof in diesem Urteil einen Alles-oder-Nichts-Ansatz: Entweder die Konvention gilt vollumfänglich oder sie gilt gar nicht.[711] Demzufolge würden nach dieser vom EGMR im Fall *Banković* vertretenen Auffassung die Verpflichtungen der EMRK nur in Fällen der umfassenden Gebietskontrolle vollumfänglich bestehen. Die Sichtweise des EGMR beruht indes darauf, dass der EGMR im Fall *Banković* allein von einer extraterritorialen Anwendbarkeit der Konvention aufgrund territorialer Kontrolle ausgeht und eine personelle Kontrolle gar nicht in Betracht zieht. In der nachfolgenden Spruchpraxis, in der auch die extraterritoriale Jurisdiktionsbegründung aufgrund personeller Kontrolle vom EGMR anerkannt wird, revidiert der Gerichtshof den Alles-oder-Nichts-Ansatz aus *Banković*.[712] Im Urteil *Al-Skeini and Others v. The United Kingdom* argumentiert der Gerichtshof wie folgt:

> „It is clear that, whenever the State, through its agents, exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms under Section I of the Convention that are relevant to the situation of that individual. In this sense, therefore, the Convention rights can be ‚divided and tailored‘ [...].“[713]

Damit bringt der Gerichtshof hier deutlich zum Ausdruck, dass der Konventionsstaat in Fällen der personellen Kontrolle nur zur Gewährung der Menschenrechte verpflichtet ist, die für das betroffene Individuum im Kontext der konkreten Jurisdiktionsumstände relevant sind.

Folglich unterscheidet der Gerichtshof zur Beurteilung des Umfangs der extraterritorialen Menschenrechtsverpflichtung zwischen Jurisdiktionsausübungen auf-

---

[710] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII.

[711] EGMR, *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII, Rn. 75. Siehe auch *Shany,* Taking Universality Seriously, S. 55.

[712] EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 137. Fraglich ist indes, warum der EGMR an dieser Stelle auf Rn. 75 des *Banković*-Urteils verweist, obwohl gerade an dieser Stelle des *Banković*-Urteils die proportionale Anpassung des Umfangs der Konventionsanwendung an das Maß der Kontrolle durch den Staat vom EGMR ausdrücklich komplett abgelehnt wird. Damit steht hier die Position des Gerichtshofs im *Al-Skeini*-Urteil im absoluten Kontrast zur *Banković*-Argumentation. Vgl. dazu auch *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg, S. 129.

[713] EGMR*, Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 137.

grund der umfassenden Gebietskontrolle und Fällen der punktuellen Kontrolle von einzelnen Individuen. Während die umfassende Gebietskontrolle demnach eine vollumfängliche Gewährleistung aller substantieller Rechte aus der EMRK nach sich zieht, beschränkt sich die Reichweite der Menschenrechtsverpflichtung im Rahmen der effektiven Kontrolle über Individuen nach Ansicht des EGMR auf das der Kontrollausübung entsprechende Maß.

Der Menschenrechtsausschuss hat sich in seiner Spruchpraxis bis dato nicht ausdrücklich dazu geäußert, ob in Fällen der Jurisdiktionsausübung aufgrund personeller Kontrolle der IPbpR nur partiell anwendbar ist. Im *General Comment* 31 ist die Verpflichtung der Staaten zur Achtung und Gewährung der Menschenrechte, die Ihnen in Fällen der extraterritorialen Jurisdiktionsausübung zukommt, zwar aufgeführt.[714] Der MRA hat die Verpflichtung der Staaten an dieser Stelle jedoch generell formuliert.[715] Aus dem *General Comment* lässt sich aus diesem Grund nicht ableiten, ob und unter welchen Voraussetzungen eine nur partielle Anwendung des IPbpR in Betracht kommt.[716] Allerdings argumentieren Literaturstimmen nicht nur hinsichtlich der EMRK, sondern auch bezüglich des IPbpR für eine partielle Verpflichtung der Staaten in Fällen der Personenkontrolle. Eines der Hauptargumente ist dabei, dass einige Menschenrechte des Paktes aufgrund ihres Wesens nicht ohne effektive Kontrolle über ein fremdes Territorium extraterritorial umgesetzt werden können.[717] So können bestimmte Menschenrechte nur dann von einem Staat auch gegenüber Individuen auf einem fremden Territorium umgesetzt werden, wenn der Staat aufgrund seiner umfassenden Territorialkontrolle Jurisdiktion über das Gebiet ausübt. So könnten etwa die Rechte aus Art. 9 und Art. 14 IPbpR nicht im Ausland umgesetzt werden, wenn ein Staat allein über einzelne Individuen extraterritoriale Jurisdiktion ausübt.[718] Denn diese Rechte erfordern naturgemäß zumindest eine effektive faktische Kontrolle über die lokalen Institutionen, die mit der Umsetzung dieser Rechte verbunden sind.[719] Ein extraterritorial agierender Staat kann demnach nicht die Anforderungen für ein faires Verfahren im Sinne des Art. 14 IPbpR verwirklichen, wenn dieser keine eingehende Kontrolle über das örtliche Justizwesen hat.[720] Vor diesem Hintergrund wird damit argumentiert, dass von den extraterritorial agierenden Staaten nicht die Umsetzung des Unmöglichen verlangt werden

[714] UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004.
[715] So heißt es hier in Rn. 10: „This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party".
[716] Vgl. auch *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 57.
[717] *King,* The Extraterritorial Human Rights Obligations of States, S. 540.
[718] *Tomuschat,* Human Rights. Between Idealism and Realism, S. 101; siehe außerdem *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 83, die zudem Art. 23 IPbpR als Beispiel benennt.
[719] *Tomuschat,* Human Rights. Between Idealism and Realism, S. 101.
[720] *King,* The Extraterritorial Human Rights Obligations of States, S. 540.

könne.[721] So kann von einem Staat, der über einzelne Individuen – etwa durch extraterritoriale Festnahmen – Jurisdiktion ausübt, nicht verlangt werden, alle Menschenrechtsbestimmungen im Aufenthaltsstaat des Individuums umzusetzen. Vielmehr kann der extraterritorial agierende Staat nur für die Umsetzung der Rechte des betroffenen Individuums verantwortlich sein, über die er aufgrund der konkreten Situation Kontrolle ausübt und die er infolgedessen auch schützen kann.[722] Das Maß der Verpflichtung des Staates hängt somit vom Umfang seiner Kontrollausübung in der entsprechenden Situation ab.

Die aufgeführten Argumente für eine partielle Geltung der Menschenrechtspflichten in Fällen der effektiven Personenkontrolle sind nicht von der Hand zu weisen. Tatsächlich muss zwischen der effektiven Gebietskontrolle und der Jurisdiktionsausübung aufgrund der Kontrolle über einzelne Personen unterschieden werden. Denn im Rahmen der umfassenden territorialen Kontrolle übt der Staat weitgehenden Einfluss auf die lokalen staatlichen Strukturen aus. Der extraterritorial agierende Staat kann sogar wie ein de-facto-Regime vor Ort durch seine faktische Machtausübung die rechtliche Hoheitsgewalt des originären Staates überwiegen. Hingegen übt ein Staat in Fällen der Personenkontrolle nur punktuell über einzelne Individuen Kontrolle und auch Hoheitsgewalt aus. Die Machtausübung und Einflussnahme des Staates betrifft nur das Individuum und berührt nicht die institutionellen Strukturen des Staates. Insofern ist nicht ersichtlich, warum der extraterritorial agierende Staat die Menschenrechtsverantwortung für jegliche Geschehnisse im fremden Staat tragen soll. Die grundsätzlich bestehende Verantwortung für Menschenrechtsverletzungen bleibt beim Heimatstaat. Der extraterritorial agierende Staat ist eben nur für die Menschenrechte verantwortlich, die in der konkreten Situation der extraterritorialen Jurisdiktionsausübung über das Individuum relevant sind. Das Maß der ausgeübten Kontrolle entscheidet über den Verpflichtungsumfang.

II. Die extraterritoriale Anwendbarkeit des IPbpR und der EMRK im Fall der extraterritorialen Telekommunikationsüberwachung

1. Problemaufriss

In Fällen der Telekommunikationsüberwachung sind extraterritoriale Konstellationen nicht nur theoretisch möglich, sondern werden von den Geheimdiensten tatsächlich in der Praxis umgesetzt. Gerade im Zeitalter der digitalen Telekommunikationstechnologie lassen sich die globalen Datenströme problemlos an allen möglichen Punkten der Welt anzapfen. Unter extraterritorialer Telekommunikationsausspähung sind letztlich all die Fälle der Korrespondenzüberwachung zu verstehen, in denen staatliche Geheimdienste grenzüberschreitend die Telekommuni-

[721] *Szydlo,* Extra-Territorial Application of the European Convention on Human Rights after Al-Skeini and Al-Jedda, S. 289.
[722] Ebd.

kation von Individuen in anderen Ländern ausspähen. Konkret können hinsichtlich der drei Grundfälle der Telekommunikationsüberwachung, die Untersuchungsgegenstand der vorliegenden Dissertation sind[723], je nach Aufenthaltsort des Individuums und des Orts der geheimdienstlichen Überwachungshandlung unterschiedliche extraterritoriale Fallkonstellationen auftreten.[724] In Fallkonstellationen der extraterritorialen Telekommunikationsüberwachung stellt sich indes die Frage, inwieweit sich das betroffene Individuum unter der Jurisdiktion des überwachenden Staates befindet. So übt der überwachende Staat allein durch den Akt der Überwachung von Individuen, die sich in einem anderen Staat befinden, keine effektive Kontrolle über das fremde Staatsgebiet aus. Es befinden sich keinerlei Organe des Staates, dessen Akte etwa dem Staat zugerechnet werden könnten, auf dem fremden Territorium. Es wird auch nicht auf sonstige Weise Kontrolle über das Territorium ausgeübt. Somit liegt kein Fall der Jurisdiktionsausübung aufgrund territorialer Kontrolle vor. Die Überwachung der Korrespondenz begründet auch keine physische Kontrolle des Staates über betroffene Individuen, sodass auch keine Jurisdiktionsausübung aufgrund personeller Kontrolle im klassischen Sinne in Betracht kommt. Auf Grundlage der bislang in der Spruchpraxis ausdrücklich anerkannten Fallgruppen der extraterritorialen Jurisdiktionsausübung – nämlich der effektiven territorialen und personellen Kontrolle – kann somit keine Jurisdiktionsausübung des überwachenden Staates begründet werden.[725]

Eine strikte und starre Anwendung dieser bisher entwickelten Fallgruppen und Kriterien der extraterritorialen Anwendbarkeit der Menschenrechtspakte würde damit eine Lücke im internationalen Menschenrechtsschutz verursachen. Denn so könnten Staaten grenzüberschreitend Überwachungsmaßnahmen durchführen, ohne dabei an ihre aus den Pakten hervorgehenden Menschrechtsverpflichtungen gebunden zu sein. Innerstaatlich menschenrechtswidrige Überwachungsmaßnahmen könnten so ungebunden extraterritorial durchgeführt werden.[726] Nachfolgend wird einerseits dargestellt, ob und wie die Rechtsprechung und Stimmen in der Literatur das Problem der extraterritorialen Anwendbarkeit des IPbpR und der EMRK im Fall der grenzüberschreitenden Telekommunikationsüberwachung lösen. Anschließend wird ein Lösungsweg vorgestellt, der die bisherigen Kriterien der „effektiven Kontrolle“ weiterentwickelt und die extraterritoriale Anwendbarkeit der Pakte auch für Fälle extraterritorialer Überwachung begründet.

---

[723] Siehe 1. Abschnitt, Unterabschnitt B. III. 2. a.–c.

[724] Siehe dazu unten 3. Abschnitt, Unterabschnitt A. II. 4. c. bb.

[725] So auch *Rona/Aarons*: State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace, S. 508. Zur Fragestellung, inwieweit „effektive Kontrolle“ unter Art. 2 Abs. 1 IPbpR im Cyberspace ausgeübt werden kann, siehe *Peters*, Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in Miller (Hrsg.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, S. 155 f.

[726] Vgl. auch *Bignami/Resta*, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti/Nolte (Hrsg.), Community Interests Across International Law, S. 362.

2. Bisherige Spruchpraxis

a. Die Spruchpraxis des MRA

Der MRA hat für die extraterritoriale Anwendbarkeit des IPbpR eine weite Auslegung entwickelt,[727] die eine Anwendbarkeit des Paktes auch für Fälle der Telekommunikationsüberwachung nicht per se ausschließt.

Bisweilen hat der UN-Menschenrechtsausschuss noch nicht über Individualbeschwerden gegen extraterritoriale Telekommunikations-Überwachungsmaßnahmen entscheiden müssen, sodass in dieser Sache keine einschlägigen *Views* vorliegen. Allerdings hat der Ausschuss in seinen *Concluding Observations* im Rahmen der Berichtsverfahren einzelner Staaten ausdrücklich zu diesem Thema Stellung bezogen. So heißt es etwa in den *Concluding Observations* zum Staatenberichtsverfahren des Vereinigten Königreichs im Jahr 2015:

> „The Committee is concerned (a) that the Regulation of Investigatory Powers Act 2000, which makes a distinction between ‚internal' and ‚external' communications, provides for untargeted warrants for the interception of external private communications and communications data that are sent or received outside the United Kingdom without affording the same safeguards as apply to the interception of internal communications […].
>
> The State party should: (a) Review the regime regulating the interception of personal communications and the retention of communications data […] with a view to ensuring that such activities, both *within and outside the State party*, conform with its obligations under the Covenant, including article 17. In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, *regardless of the nationality or location of the individuals* whose communications are under direct surveillance".[728]

Indem der Ausschuss den Vertragsstaat hier dazu anhält, die nationalen Regulierungen zur Telekommunikationsüberwachung auch hinsichtlich extraterritorialer Überwachungsmaßnahmen mit dem Pakt in Einklang zu bringen, lässt er eindeutig verlauten, dass die Verpflichtungen aus dem IPbpR auch für Auslandsüberwachungen gelten. So müssten die Grundsätze des Schutzes der Privatsphäre aus Art. 17 IPbpR für jegliche Überwachungsmaßnahmen beachtet werden, ohne dass es dabei auf den Aufenthaltsort des Individuums ankomme. Der Schutz der Privatsphäre gemäß Art. 17 IPbpR gilt damit nach Ansicht des Ausschusses auch für extraterritoriale Überwachungsmaßnahmen. In ähnlicher Weise hat der Ausschuss diesen

[727] Siehe dazu ausführlich 3. Abschnitt, Unterabschnitt A. I. 1. a. aa.

[728] UN Human Rights Committee, Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24 [Hervorh. d. Verf.].

Standpunkt 2014 auch in den *Concluding Observations* der USA formuliert.[729] Bereits 2006 hat der Ausschuss schon Bedenken hinsichtlich der grenzüberschreitenden Überwachungsmaßnahmen der USA geäußert, allerdings ist hier die Ausdrucksweise des Ausschusses noch deutlich zurückhaltender.[730] Immerhin zeigt dies aber, dass der Menschenrechtsausschuss schon damals die extraterritoriale Telekommunikationsüberwachung als menschenrechtliches Problem identifiziert hat.

Die dargelegten Stellungnahmen des Ausschusses in diesen *Concluding Observations* belegen allerdings nur, dass er im Ergebnis eine extraterritoriale Anwendbarkeit des Paktes in Fällen der extraterritorialen Überwachung prinzipiell befürwortet. Sie geben jedoch keinen Aufschluss darüber, wie der Ausschuss diesen Standpunkt begründet.[731] Wie etwa die bislang entwickelten Kriterien der Jurisdiktionsausübung im Sinne des Art. 2 Abs. 1 IPbpR im Fall der Telekommunikationsüberwachung anzuwenden sind und inwiefern ein Staat in solchen Überwachungsfällen „effektive Kontrolle" ausübt, bleibt offen.

In seinem Bericht zum Schutz der Privatsphäre im digitalen Zeitalter hat der OHCHR die extraterritoriale Anwendbarkeit des IPbpR in Fällen der grenzüberschreitenden Telekommunikationsüberwachung befürwortet. Voraussetzung hierfür sei indes die Ausübung effektiver Kontrolle über die digitale Telekommunikationsinfrastruktur.[732]

b. Die Spruchpraxis des EGMR

Obwohl die Spruchpraxis des EGMR zur Vereinbarkeit geheimdienstlicher Überwachungsmaßnahmen mit der EMRK umfangreich ist, hat der Gerichtshof bislang kein Urteil gefällt, das sich ausführlich mit der extraterritorialen Anwendung der Konvention im Fall der extraterritorialen Telekommunikationsüberwachung befasst. Dabei lag dem Fall *Weber and Saravia v. Germany* durchaus ein extraterritorialer Überwachungssachverhalt zugrunde. So haben die beiden in Uruguay ansässigen

---

[729] UN Human Rights Committee, Concluding observations: USA, CCPR/C/USA/CO/4, 23. April 2014, Rn. 22. Außerdem auch UN Human Rights Committee, Concluding observations: France, CCPR/C/FRA/CO/5, 17. August 2015, Rn. 12; Concluding observations: Norway, CCPR/C/NOR/CO/7, 25. April 2018, Rn. 21.

[730] UN Human Rights Committee, Concluding observations: USA, CCPR/C/USA/CO/3/Rev.1, 18. Dezember 2006, Rn. 21.

[731] Vgl. auch den Beitrag von *Neuman, Gerald*: Has the Human Rights Committee Extended its Reach?, Just Security, 29. Juli 2015, abrufbar unter: https://www.justsecurity.org/25022/human-rights-committee-extended-reach/ [zuletzt abgerufen: 02.12.2021].

[732] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 34. Auch in dem neuen Bericht von 2018 vertritt der OHCHR weiterhin diese Auffassung, siehe Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 9: „Human rights law applies where a State exercises its power or effective control in relation to digital communications infrastructure, wherever located, for example through direct tapping or penetration of communications infrastructure located outside the territory of that State." Dazu kritisch *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 145.

Beschwerdeführer dieses Falles eine Verletzung von Art. 8 EMRK aufgrund der Bestimmungen im deutschen G-10-Gesetzes gerügt, die eine Überwachung des internationalen Telekommunikationsverkehrs durch die zuständigen deutschen Behörden regulieren.[733] Der EGMR beantwortete allerdings die Frage nach der Jurisdiktionsausübung Deutschlands über die Beschwerdeführer nicht, da er die Beschwerde wegen offensichtlicher Unbegründetheit zurückwies.[734]

Auch in der Entscheidung des EGMR im Fall *Big Brother Watch and Others v. The United Kingdom*[735] war die extraterritoriale Anwendbarkeit der Konvention in Fällen der Telekommunikationsüberwachung nicht Gegenstand der durchaus umfassenden rechtlichen Überprüfung. Dabei hätte der Beschwerdegegenstand durchaus Anlass hierfür geben können. In diesem Fall machen die Beschwerdeführer, die teilweise ihren Sitz in Großbritannien und anderen europäischen Staaten haben und zum Teil außerhalb Europas ansässig sind, nämlich geltend, dass die internationalen Überwachungsmaßnahmen britischer Behörden (z.B. das „*TEMPORA*"-Programm[736]) ihre Rechte aus Art. 8 EMRK und Art. 10 EMRK verletzen.

Des Weiteren betreffen die Fälle auch die von der NSA durchgeführten Programme „*PRISM*" und „*UPSTREAM*", da die Beschwerdeführer geltend machen, dass Großbritannien die aus diesen Programmen gewonnenen Informationen von den USA erhält und für eigene Zwecke nutzt. Sie richten sich somit gegen die durch das Vereinigte Königreich selbst durchgeführten Überwachungsmaßnahmen als auch gegen den Erhalt geheimdienstlicher Informationen über Individuen, die wiederum von ausländischen Überwachungsbehörden gesammelt wurden. Die Große Kammer stellt in dem Urteil vorab folgendes fest:

> „In respect of the section 8(4) regime, the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the Government expressly confirmed that they had raised no objection on this ground as at

---

[733] EGMR, *Weber and Saravia v. Germany*, Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 63ff.

[734] Ebd., Rn. 72 und Rn. 138. Der Gerichtshof äußert sich in diesem Fall knapp zur Frage des grenzüberschreitenden Charakters der Überwachungsmaßnahmen: „The Court observes that the impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law", EGMR, *Weber and Saravia v. Germany*, Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI, Rn. 88.

[735] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021.

[736] Siehe 1. Abschnitt, Unterabschnitt B. III. 2. a.

> least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the section 8(4) regime, the matters complained of fell within the jurisdictional competence of the United Kingdom."[737]

Auch in diesem Urteil findet eine Überprüfung der extraterritorialen Jurisdiktionsausübung der überwachenden Staaten somit nicht statt.

c. Zwischenergebnis

Der MRA und der EGMR sind erst in jüngerer Zeit mit der Frage der extraterritorialen Anwendbarkeit der Menschenrechtspakte im Fall der digitalen Telekommunikationsüberwachung konfrontiert. Somit hatten sie noch nicht die Gelegenheit dazu, im Rahmen ihrer Spruchpraxis ihre Sichtweise zu dieser Fragestellung vollumfänglich auszuführen. Der Menschenrechtsausschuss hat immerhin im Rahmen der Staatenberichtsverfahren zu der Praxis extraterritorialer Telekommunikationsüberwachung einzelner Staaten Stellung beziehen müssen und die extraterritoriale Anwendbarkeit des IPbpR im Ergebnis grundsätzlich befürwortet. Der EGMR hat sich in seiner Jurisprudenz bislang noch nicht zu dieser Fragestellung geäußert. Angesichts der jüngsten Beschwerden gegen grenzüberschreitende Überwachungsprogramme Großbritanniens – ausgelöst durch die *Snowden*-Enthüllungen – war wohl teilweise eine Stellungnahme des Gerichtshofs erwartet worden.[738] Die Jurisdiktionsausübung wurde aber im Urteil letztlich nicht vertieft problematisiert.

3. Begründungsansätze in der Literatur

Die *Snowden*-Enthüllungen haben nicht nur eine Welle von Individualbeschwerden beim EGMR ausgelöst.[739] Auch in der Wissenschaft wird seitdem diskutiert, inwieweit grenzüberschreitende Telekommunikationsüberwachungsmaßnahmen mit dem internationalen Menschenrechtsschutz vereinbar sind.[740] Im Fokus dieser Diskussionen steht insbesondere auch die Frage, ob und unter welchen Voraussetzungen internationale Menschrechtspakte in diesen Fällen extraterritorial anwendbar sind. Dabei haben einige Wissenschaftler unterschiedliche Konzeptionen zur

---

[737] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 272.

[738] Vgl. auch die Einschätzung von *Watt,* The right to privacy and the future of mass surveillance, S. 778.

[739] Das Urteil *Big Brother Watch and Others v. The United Kingdom* basiert auf drei getrennten Beschwerden (Beschwerdenummern: 58170/13; 62322/14; 24960/15), die zeitnah beim EGMR eingingen und aufgrund ihrer inhaltlichen Ähnlichkeit vom Gerichtshof zusammengefasst wurden.

[740] Siehe etwa *Margulies,* The NSA in Global Perspective, S. 2150 f; *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 120 ff.; *Bignami/Resta*, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti/Nolte (Hrsg.), Community Interests Across International Law, S. 3 ff.

Begründung der Jurisdiktionsausübung der Staaten in Fällen der grenzüberschreitenden Überwachung der Telekommunikation entwickelt. Eine beispielhafte Auswahl dieser unterschiedlichen Begründungsansätze wird im Folgenden zusammengestellt.

Die unterschiedlichen Ansichten unter den Literaturstimmen basieren allesamt auf der Prämisse, dass die bislang von den internationalen Menschenrechtsorganen entwickelten Jurisdiktionskriterien für eine extraterritoriale Anwendbarkeit der Menschenrechtsverträge grenzüberschreitende Maßnahmen zur Telekommunikationsüberwachung nicht erfassen können. So stellt auch *Margulies* eindeutig fest, dass die bisherigen Kriterien – die personelle und territoriale Kontrolle – für die Cybersphäre nicht anwendbar und unzureichend sind.[741] Vor diesem Hintergrund stellt er hinsichtlich der Anwendbarkeit des IPbpR die Konzeption der *virtuellen* Kontrolle als Lösung dieses Problems vor:

> „A narrow standard requiring physical control does not do justice to the challenge of rapidly evolving technology in a changing world. The virtual control test supplies a broader standard that meets this challenge."[742]

Demnach müsse angesichts der technologischen Entwicklungen der modernen Welt eine Erweiterung der bisherigen Kriterien der extraterritorialen Jurisdiktionsausübung in Form einer virtuellen Kontrolle vorgenommen werden. Mit ähnlicher Argumentation stellt *Peters* ebenso fest, dass im *cyber-age* eine Begründung von extraterritorialen Menschenrechtsverpflichtungen aufgrund virtueller Kontrolle nicht weit hergeholt sei.[743] Auch *Georgieva* unterstützt die Konzeption der virtuellen Kontrolle und führt als bekräftigendes Argument hinzu, dass diese Theorie sehr nahe an der bisher von den internationalen Spruchkörpern entwickelten Konzeption der effektiven Kontrolle liegt.[744] Tatsächlich scheint die Grundidee der virtuellen Kontrolle als Konzeptionsansatz eine angemessene Modernisierung und Erweiterung der „*effective control*"-Konzeption darzustellen. Allerdings führen die Befürworter des Konzeptes nicht näher aus, unter welchen Voraussetzungen ein Staat virtuelle Kontrolle über ein Individuum ausübt. Letztlich muss anhand konkreter Kriterien bestimmbar sein, ab wann von virtueller Kontrolle gesprochen werden kann. *Margulies* stellt zwar am konkreten Beispiel der enthüllten NSA-Überwachungsmaßnahmen fest, dass die USA aufgrund des Mithörens, Filterns und sogar Veränderns der Telekommunikationsdaten virtuelle Kontrolle ausgeübt haben.[745] Nichtsdestotrotz

---

[741] *Margulies,* The NSA in Global Perspective, S. 2150 f.
[742] Ebd., S. 2152.
[743] *Peters, Anne*: Surveillance without Borders. The Unlawfulness of the NSA Panopticon, Part II, EJIL: Talk!, Blog of the European Journal of International Law, 4. November 2013, abrufbar unter: https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ [zuletzt abgerufen: 02.12.2021].
[744] *Georgieva,* The Right to Privacy under Fire, S. 113.
[745] *Margulies,* The NSA in Global Perspective, S. 2151 f.

bleibt die Frage offen, wie generell bestimmt werden kann, ob im Einzelfall virtuelle Kontrolle zur Begründung einer extraterritorialen Jurisdiktionsausübung vorliegt.

Auch *Milanovic* hat die Frage nach der extraterritorialen Anwendbarkeit des IPbpR und der EMRK im Fall der grenzüberschreitenden Telekommunikationsüberwachung untersucht und eine ganz andere Antwort entwickelt.[746] Ausgangspunkt *Milanovics* ist die von ihm eigens konzipierte Unterscheidung zwischen negativen und positiven Pflichten im Rahmen der allgemeinen extraterritorialen Anwendbarkeit von Menschenrechtspakten. Danach sei die Frage nach der Ausübung effektiver Kontrolle allein für die positiven Pflichten der Staaten relevant, während die negativen Pflichten in jedem Fall und territorial unbegrenzt sowohl in nationalen als auch extraterritorialen Sachverhalten zu achten seien.[747] Auf dieser Grundlage stellt *Milanovic* fest, dass in Überwachungsfällen die Menschenrechtsverträge in jedem Fall anwendbar sind, da die Staaten durch Überwachungsmaßnahmen ihre negativen Pflichten verletzen. Als Hauptargument für diese Theorie führt *Milanovic* aus, dass die strikte Anwendung der anerkannten Konzeption effektiver personeller oder territorialer Kontrolle zu willkürlichen Ergebnissen führen würde.

Teilweise wird auch die Auffassung vertreten, dass die Staaten in Fällen der extraterritorialen Telekommunikationsüberwachung über das Recht der Privatsphäre betroffener Individuen Kontrolle ausüben.[748] Diese Konzeption der „*authority and control over an individual's rights*" leiten sie unterdies aus der Spruchpraxis des EGMR in Fällen der Jurisdiktionsausübung aufgrund gezielter Tötungen[749] ab. So zeigten die EGMR-Entscheidungen *Pad and Others v. Turkey*[750] und *Jaloud v. The Netherlands*[751], dass der Gerichtshof in diesen Fällen dazu tendiere, die Jurisdiktionsausübung der Staaten anhand einer ferngesteuerten Kontrolle des Rechts auf Lebens

[746] *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 120 ff.

[747] *Milanovic* unterscheidet zwischen negativen und positiven Pflichten der Paktstaaten. So verweist er auf den Wortlaut von Art. 1 EMRK, der allein das Verb „secure" enthält. Des Weiteren könne der Wortlaut des Art. 2 Abs. 1 IPbpR so ausgelegt werden, dass sich der Begriff „jurisdiction" allein auf das Verb „ensure" und nicht auf „respect" beziehe. Daraus folge, dass die negativen Pflichten der jeweiligen Vertragsstaaten, menschenrechtsverletzende Handlungen zu unterlassen, nicht den Jurisdiktionsklauseln der beiden Pakte unterliegen. Vielmehr seien die Staaten überall – d.h. territorial ungebunden – an ihre negativen Menschenrechtsverpflichtungen gebunden, ohne dass es dabei auf die Ausübung von Jurisdiktion im Sinne der Art. 2 Abs. 1 IPbpR und Art. 1 EMRK ankäme. Allein die positiven Pflichten der Staaten, d.h. die Schutzpflichten, unterliegen den Jurisdiktionsklauseln, da ihnen nicht zugemutet werden könne, grenzenlos weltweit menschenrechtliche Schutzpflichten zu erfüllen. Damit sei das Prinzip der Universalität der Menschenrechte gebührend gewahrt, während die weitreichenden positiven Pflichten der Staaten unter der Voraussetzung der Jurisdiktionsausübung sinnvoll begrenzt würden. Siehe dazu *Milanovic,* Extraterritorial Application of Human Rights Treaties, S. 209 ff.; *Milanovic*, Human Rights Treaties and Foreign Surveillance, S. 119.

[748] Vgl. *Ng, Vivian/Murray, Daragh*: Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?, Human Rights Centre Blog (University of Essex), 2. August 2016, abrufbar unter: https://hrcessex.wordpress.com/2016/08/02/extraterritorial-human-rights-obligations-in-the-context-of-state-surveillance-activities/ [zuletzt abgerufen: 02.12.2021].

[749] Siehe hierzu bereits oben 3. Abschnitt, Unterabschnitt A. 2. b. bb. (2).

[750] *Pad and Others v. Turkey,* Rs. 60167/00, 28. Juni 2007.

[751] *Jaloud v. The Netherlands* [GC], Rs. 47708/08, 20. November 2014, Rep. 2014.

zu begründen. Diese Annahme übertragen sie schließlich auf die Telekommunikationsüberwachung. Indem die Staaten die Telekommunikation von Individuen, die sich außerhalb des eigenen Staatsgebiets befinden, abgehört, gespeichert und verarbeitet haben, übten sie demzufolge effektive Kontrolle über das Recht auf Privatsphäre der betroffenen Personen aus. Der Ansatz dieser Konzeption ist durchaus interessant, allerdings stellt sich die ungeklärte Anschlussfrage, wann und unter welchen Voraussetzungen ein Staat über diese Rechte Kontrolle ausüben kann.

4. *Effektive Kontrolle über ein Schutzobjekt – eine neue Fallgruppe der extraterritorialen Jurisdiktionsausübung*

Die bisherigen Fallgruppen und Kriterien, die von der internationalen Rechtsprechung zur extraterritorialen Anwendbarkeit von Menschenrechtspakten entwickelt wurden, orientieren sich freilich an den Sachlagen, mit denen die Spruchkörper bislang konfrontiert waren und zu entscheiden hatten. Grenzüberschreitende Telekommunikationsüberwachung ist erst in den vergangenen Jahren zum Thema innerhalb der internationalen Menschenrechts-Jurisprudenz geworden, wobei eine ausführliche Spruchpraxis zu diesem Thema noch fehlt.[752] Das Konzept der effektiven territorialen und personellen Kontrolle zur Begründung extraterritorialer Jurisdiktionsausübung hat zur Folge, dass Lücken im internationalen Menschenrechtsschutz vermieden werden. Die Unanwendbarkeit der bislang anerkannten Kriterien extraterritorialer Jurisdiktionsausübung auf das Phänomen moderner Überwachungssysteme darf nicht zur Schussfolgerung führen, dass grenzüberschreitende Telekommunikationsüberwachung *a priori* keine extraterritoriale Anwendung der Menschenrechtspakte auslöse. Der technische Fortschritt der Telekommunikation erfordert gleichermaßen im Sinne der Lückenlosigkeit und Universalität des internationalen Menschenrechtsschutzes eine adäquate Modernisierung der bislang anerkannten Kriterien extraterritorialer Jurisdiktionsausübung. So muss gefragt werden, wie angesichts dieses modernen Phänomens die bisherige Rechtsprechung der extraterritorialen Anwendbarkeit von internationalen Menschenrechtsverträgen weiterentwickelt werden kann. Die oben dargestellten Ansichten der Literatur liefern bereits einige Ansätze zur Beantwortung dieser Fragestellung.

Anknüpfend an die bisherige Rechtsprechung zur Extraterritorialität der Pakte und den vorgestellten Ansätzen innerhalb der Literatur wird an dieser Stelle nun eine neue Fallgruppe der extraterritorialen Anwendbarkeit des IPbpR und der EMRK konzipiert. Diese Fallgruppe soll all die extraterritorialen Handlungen von Staaten erfassen, die weder eine Kontrolle des Territoriums noch der Individuen selbst begründen, sondern vielmehr eine Kontrolle über bestimmte Objekte verursachen. Eine extraterritoriale Kontrolle über diese Objekte – im folgenden „Schutzobjekte" – durch einen Staat kann indes die freie und menschenrechtlich geschützte Rechtsausübung an diesen Objekten beeinträchtigen, sodass aufgrund

[752] Siehe vorangegangenen Unterabschnitt A. II. 2.

dieser „Objektskontrolle“ die extraterritoriale Jurisdiktionsausübung des Staates begründet wird. Was konkret unter „Schutzobjekt“ zu verstehen ist und inwieweit ein Staat effektive Kontrolle über diese Schutzobjekte ausüben und dadurch extraterritoriale Jurisdiktion begründen kann, wird nachfolgend dargelegt.

a. Schutzobjekt: Begriff und Beispiele

Der Begriff „Schutzobjekt“ bezeichnet im Rahmen der vorliegenden Dissertation all die Objekte, an denen Individuen aufgrund der Menschenrechtspakte geschützte Rechte haben. Die grundlegenden Menschenrechte schützen zwar überwiegend Individualrechtsgüter, die nicht vom Individuum trennbar sind, wie etwa das Recht auf Leben, die persönliche Freiheit oder die Freiheit der Religionsausübung. Daneben bezieht sich der Schutzbereich einzelner Menschenrechte jedoch auch auf bestimmte Schutzobjekte. Die Menschenrechtspakte schützen dabei zwar keine Objekte vor staatlichen Handlungen – Objekte sind in diesem Sinne gewiss keine Menschenrechtsträger. Allerdings wird das Recht der Individuen an bestimmten Objekten, die vom Individuum körperlich abtrennbar sind und zu denen das Individuum einen menschenrechtlich relevanten Bezug hat, geschützt.

So wird beispielsweise die Unverletzlichkeit der Wohnung in Art. 17 IPbpR und Art. 8 EMRK gewährt. Dieses Menschenrecht schützt die berechtigten Individuen vor staatlichen Eingriffen etwa in Form von unrechtmäßigen Wohnungsdurchsuchungen oder Zwangsräumungen.[753] Schutzobjekt dieses Menschenrechts ist die Wohnung, die selbstverständlich vom Individuum abtrennbar ist. Auch in Abwesenheit der Bewohner kann beispielsweise eine willkürliche Durchsuchung der Wohnung vorgenommen werden und damit eine Verletzung dieses Rechts durch staatliches Handeln erfolgen.

Als weiteres Beispiel kann der Schutz des Eigentums genannt werden, denn auch das Eigentum bezieht sich auf vom Individuum trennbare Schutzobjekte. Problematisch ist an diesem Beispiel jedoch, dass der Schutz des Eigentums nicht in allen Pakten als Menschenrecht kodifiziert ist. Die AEMR benennt in Art. 17 zwar das Recht auf Eigentum, der IPbpR enthält diese Garantie indes nicht.[754] Auch in die EMRK selbst hat diese Garantie keinen Einzug gefunden, die Achtung des Eigentums wird aber in Art. 1 des ersten Zusatzprotokolls zur EMRK von 1954 gewährleistet.[755] Enteignungen oder Nutzungsverweigerungen – etwa eines Grund-

[753] *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 473.
[754] Dies bedeutet jedoch nicht, dass das Eigentum keinerlei Schutz durch den IPbpR erfährt. Zu diesem Thema, dessen eingehende Ausarbeitung an dieser Stelle den Rahmen der vorliegenden Arbeit sprengen würde, siehe insbesondere *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 531 ff. Hier wird dargestellt, dass aus einigen Garantien des Paktes ein indirekter Schutz des Eigentums folge, wobei insbesondere Art. 17 IPbpR „ein Potenzial zum Schutz gewisser Aspekte des Eigentumsrechts“ besitze. Siehe außerdem UN Human Rights Committee, *Simunek v. Czech Republic,* No. 516/1992, CCPR/C/54/D/516/199, 19. Juli 1995.
[755] Siehe oben Fn. 576.

stücks – durch den Staat stellen einen Eingriff in den Schutz des Eigentums dar.[756] Auch in diesem Fall hängt eine Verletzung dieses Rechts nicht von der örtlichen Anwesenheit der Eigentümer ab.

Im Rahmen des Schutzes der Korrespondenz gemäß Art. 17 IPbpR sowie Art. 8 EMRK ist einerseits hinsichtlich der klassischen Briefkorrespondenz der abgesendete Brief ein Schutzobjekt. Dieses Menschenrecht auf Vertraulichkeit der Korrespondenz wird klassischerweise in Abwesenheit des Individuums verletzt, indem etwa der Brief auf dem Weg zum Empfänger von staatlichen Organen abgefangen und eingesehen wird. Darüber hinaus sind aber auch Datenpakete, die aufgrund moderner, digitaler Formen der Korrespondenz abgesendet werden, als Schutzobjekte einzustufen. Der hier verwendete Begriff „Schutzobjekt" ist nämlich nicht auf körperliche Sachen begrenzt, sondern umfasst auch Daten als immaterielle Rechtsobjekte.[757] Dies ist nicht nur für den Schutz der Korrespondenz relevant, sondern betrifft auch den allgemeinen Schutz personenbezogener Daten gemäß Art. 17 IPbpR sowie Art. 8 EMRK.[758] So sind auch personenbezogene Daten, die etwa auf offiziellen Datenbanken gespeichert werden und sich oftmals außerhalb der Zugriffsreichweite betroffener Individuen befinden, Schutzobjekte. Denn insbesondere Daten sind in der Regel auf bestimmte Datenträger oder Datenbanken gespeichert und eben nicht direkt mit dem Individuum verbunden. Verschafft sich beispielsweise ein Staat unberechtigterweise Zugriff auf die Patientendaten einer Person, die in der Datenbank eines Klinikums archiviert sind, so liegt ein Eingriff in das Recht auf Schutz der personenbezogenen Daten vor. Eine derartige Rechtsverletzung geschieht fernab des Individuums, das selbst ohne Informationen von außen niemals von dieser Eingriffshandlung erfahren würde.

b. Jurisdiktionsausübung aufgrund effektiver Kontrolle über Schutzobjekte

aa. Die Grundkonzeption

Die extraterritoriale Jurisdiktionsausübung eines Staates kann auch aufgrund der effektiven Kontrolle über menschenrechtlich relevante Schutzobjekte begründet werden. Das Konzept der Schutzobjektskontrolle erfasst dabei letztlich all die extraterritorialen Handlungen von Staaten, die weder eine Kontrolle des Territoriums noch der Individuen selbst begründen, sondern vielmehr eine Kontrolle über bestimmte Objekte verursachen.

Durchsucht ein Staat etwa in einem extraterritorialen Kontext eine private Wohnung oder fängt er private Briefkorrespondenzen ab, so übt er keine Gewalt über

[756] Ein passendes Beispiel hierfür ist die EGMR-Entscheidung im Fall *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI.
[757] *Unseld,* Die Kommerzialisierung personenbezogener Daten, S. 39; *Zech,* Information als Schutzgegenstand, S. 178.
[758] Zum Schutz der personenbezogenen Daten siehe oben 2. Abschnitt, Unterabschnitte A. I. 2. d. und A. II. 2. c.

die Personen aus. Jedoch befinden sich die Wohnung und die Briefe – zumindest für einen bestimmten Zeitraum – in der staatlichen Gewalt. Ausgehend vom oben dargestellten Jurisdiktionsbegriff beruht in diesen Fällen die Jurisdiktionsbeziehung zwischen dem Staat und den betroffenen Individuen mithin auf der extraterritorialen staatlichen Gewalt über die Schutzobjekte.[759] Konkret besteht der *„jurisdictional link"* für den konkreten Zeitraum, in dem der Staat effektive Kontrolle über die Schutzobjekte ausübt. Denn durch diese Kontrolle wird die von den Menschenrechtspakten geschützte Rechtsposition der Individuen als Bewohner oder als Korrespondenzbeteiligte nicht unerheblich beeinträchtigt. Das Wesen dieser Menschenrechte, die sich auf Schutzobjekte beziehen, bringt es eben mit sich, dass staatliche Verletzungshandlungen auch in Abwesenheit der Individuen geschehen können. In manchen Fällen – etwa hinsichtlich der Überwachung von Korrespondenzen – wird der staatliche Akt in aller Regel fernab des Individuums und sogar seines Wissens vorgenommen. Dabei wiegen solche extraterritorialen Verletzungshandlungen – wie Wohnungsdurchsuchungen oder Korrespondenzüberwachungen – nicht per se weniger schwer als etwa extraterritoriale Festnahmen. Der Unterschied besteht einzig darin, dass manche Rechte, wie etwa das Recht auf persönliche Freiheit, zwangsläufig durch physische Kontrolle tangiert werden können, während andere Rechte, wie das Recht auf Schutz der personenbezogenen Daten, auch ohne physisches Element verletzt werden können. Ob sich die extraterritoriale Hoheitsgewalt nun aufgrund des Wesens der in Frage stehenden Menschenrechte auf das Individuum in physischem Sinne erstrecken kann, darf nicht das entscheidende Kriterium für das Vorliegen einer extraterritorialen Menschenrechtsverletzung sein. Anderenfalls würden extraterritoriale Korrespondenzüberwachungen nie zu einer Anwendbarkeit der Menschenrechtspakte führen. Dieses Ergebnis wäre freilich willkürlich. Vielmehr muss im Grundsatz für die extraterritoriale Jurisdiktionsbegründung die staatliche Gewalt über Schutzobjekte dem Fall der staatlichen Gewalt über Individuen gleichgestellt werden. Führt die effektive Kontrolle über Individuen zu einer extraterritorialen Anwendbarkeit der Menschenrechtsverpflichtungen, so muss dies im Ergebnis gleichermaßen für die effektive Kontrolle über menschenrechtlich relevante Schutzobjekte gelten.

Dabei stellt sich an dieser Stelle die Frage, wann ein Staat überhaupt über ein Schutzobjekt *effektive Kontrolle* ausübt. Die bisherige Rechtsprechung der territorialen und personellen Kontrolle kann hier durchaus sinngemäß übertragen werden. Wie oben dargestellt, ist die militärische Besetzung eines States der typische Fall extraterritorialer Jurisdiktionsausübung aufgrund territorialer Kontrolle. Kernkriterium der extraterritorialen personellen Kontrolle ist wiederum die unmittelbare Ausübung physischer Gewalt und Kontrolle über Individuen. Gemeinsames Merkmal beider Fallgruppen ist die – entweder ausschließliche oder zumindest überwiegende – Einflussnahme des agierenden Staates über das fremde Territorium oder über das betroffene Individuum. Besetzt etwa Staat X das Territorium des Staates Y, so führt

[759] Siehe zum Jurisdiktionsbegriff oben 3. Abschnitt, Unterabschnitt A. I. 1.

die militärische Besetzungsgewalt zumindest zu einer erheblichen Minimierung der faktischen Hoheitsgewalt des Staates Y auf seinem eigenen Staatsgebiet. In den meisten Fällen wird der Besatzungsstaat wohl ausschließliche Kontrolle über das Territorium ausüben, während der Staat selbst über keinerlei Kontrolle mehr über sein Staatsgebiet verfügt. Auch im Fall der personellen Kontrolle – etwa in Form einer extraterritorialen Festnahme – befindet sich das Individuum häufig zumindest zeitweise im exklusiven Einflussbereich des extraterritorial agierenden Staates.[760] Der Staat, auf dessen Territorium die Verletzungshandlung vorgenommen wird, hat hingegen während dieses Zeitraums oftmals keinerlei Einfluss mehr auf das Individuum.[761] Eine effektive Kontrolle über ein Schutzobjekt liegt demzufolge vor, wenn sich das Schutzobjekt zumindest zeitweise im Einflussbereich des extraterritorial agierenden Staates befindet. Die Einflussnahme kann dabei ausschließlich sein, sodass der Staat, in dem sich das Schutzobjekt befindet, in dieser Zeitspanne keinerlei Einfluss mehr auf das Objekt verfügt. Die Einflussnahme und die Gewaltausübung des Staates über die Schutzobjekte begründen die faktische Kontrolle durch den Staat. Aufgrund dieser faktischen Kontrolle übt der Staat Jurisdiktion über die Schutzobjekte aus.

bb. Die Schutzobjektskontrolle im Lichte der bisherigen Spruchpraxis des MRA und des EGMR

Das Konzept der extraterritorialen Jurisdiktionsausübung aufgrund effektiver Kontrolle über Schutzobjekte geht bis dato nicht direkt aus der Spruchpraxis des MRA sowie des EGMR hervor. Aus diesem Grund soll an dieser Stelle die Frage im Fokus stehen, inwieweit das dargestellte Konzept der Schutzobjektskontrolle mit der bisherigen Jurisprudenz zur extraterritorialen Anwendbarkeit der Menschenrechtspakte im Einklang steht.

Der Menschenrechtsausschuss hat in seiner Spruchpraxis sehr deutlich zum Ausdruck gebracht, dass extraterritoriale Verletzungshandlungen eine Anwendung des IPbpR begründen. Die offene und flexible Haltung des Ausschusses hinsichtlich der extraterritorialen Anwendbarkeit des Paktes wurde oben bereits anhand *General Comment* 31, einschlägiger *Views* sowie *Concluding Observations* ausführlich dargestellt.[762] Insbesondere sei an dieser Stelle erneut hervorgehoben, dass nach Ansicht des Menschenrechtsauschuss für die Jurisdiktionsbegründung allein das Verhältnis zwischen dem Individuum und dem Staat hinsichtlich der geschehenen Menschenrechtsverletzung entscheidend ist. Der Ort der Verletzungshandlung spiele dabei keine Rolle.[763] Der Ausschuss hat an seine weite Auslegung des Jurisdiktionsbegriffs

[760] Siehe hierzu außerdem *Margulies,* The NSA in Global Perspective, S. 11.
[761] Siehe dazu etwa die Fälle der extraterritorialen Inhaftierung, dazu ausführlich 3. Abschnitt, Unterabschnitt A. I. 2. b. bb. (1).
[762] Siehe 3. Abschnitt, Unterabschnitte A. I. 1. a. aa. und A. I. 2. a.–b.
[763] Vgl. UN Human Rights Committee, *Lopez Burgos v. Uruguay*, No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981, Rn. 12.2.

über die Jahre beibehalten. Insbesondere hat er seine Sichtweise über die extraterritoriale Anwendbarkeit des IPbpR auch nicht abschließend auf konkrete Fallgruppen begrenzt. So wurde selbst die Anwendung der Paktbestimmungen im Ergebnis für die Fälle der extraterritorialen Telekommunikationsüberwachung prinzipiell befürwortet. Damit steht die Spruchpraxis des Menschenrechtsausschusses dem Konzept der Schutzobjektskontrolle nicht entgegen. Vielmehr sprechen die Argumente des Ausschusses, die er generell für die extraterritoriale Anwendbarkeit des Paktes anführt, auch für den Grundgedanken der Schutzobjektstheorie. So argumentiert der Ausschuss einerseits ergebnisorientiert. Denn nach Ansicht des Ausschusses, dürften innerstaatliche Verletzungshandlungen nicht außerhalb der Staatsgrenzen legitim sein.[764] Aber genau dies wäre die Folge, wenn man für die Jurisdiktionsbegründung strikt auf eine physische Kontrolle über das Individuum selbst abstellen würde. Denn die schutzobjektsbezogenen Menschenrechte können durchaus ohne Kontrolle über die Individuen verletzt werden. Zudem entsteht das nach Ansicht des Ausschusses entscheidende Jurisdiktionsverhältnis zwischen dem Individuum und dem Staat auch, wenn der Staat menschenrechtlich relevante Schutzobjekte kontrolliert und auf diesem Wege Menschenrechte verletzt.

Der EGMR ist dahingegen in der Auslegung der Jurisdiktionsklausel in Art.1 EMRK deutlich strenger. Denn nach Ansicht des Gerichtshofs wird Jurisdiktion vorrangig auf dem territorialen Hoheitsgebiet eines Staates ausgeübt und nur in einzelnen Ausnahmefällen komme eine extraterritoriale Hoheitsgewalt in Betracht.[765] Auf den ersten Blick liegt die Schlussfolgerung insofern nahe, dass das Konzept der Schutzobjektskontrolle mit der engen Auslegung des EGMR in seiner bisherigen Spruchpraxis nicht im Einklang steht. Allerdings verbirgt sich in der Leitentscheidung *Loizidou v. Turkey* ein Ansatz, der die Jurisdiktionsbegründung aufgrund einer extraterritorialen Schutzobjektskontrolle unterstützt.[766] So ist in dieser bereits in den 90er Jahren ergangenen Entscheidung die zugrundeliegende Dreieckskonstellation des Sachverhaltes interessant. Die Türkei übt hier effektive Gesamtkontrolle über den nordzypriotischen Landesteil aus. Die Beschwerdeführerin befindet sich jedoch im südzypriotischen Teil. Allein ihre Grundstücke befinden sich in Nordzypern und damit auf dem Gebiet, das aufgrund der territorialen effektiven Gesamtkontrolle in die Jurisdiktion der Türkei fällt. Bezugspunkt der Jurisdiktion im Sinne des Art. 1 EMRK ist hier somit nicht das Rechtssubjekt selbst, das sich gar nicht auf dem kontrollierten Gebiet befindet, sondern vielmehr die Grundstücke, auf die sich die Eigentumsrechte des Rechtssubjekts beziehen.[767] Der Gerichtshof kam hier zu dem Ergebnis, dass die Zugangsverweigerung zu den Grundstücken und der infolgedessen erlittene Verlust der Ausübung von Eigentumsrechten in die Jurisdiktion der Türkei fielen. Das Grundkonzept der Schutzobjektstheorie lässt sich in der

[764] Siehe oben 3. Abschnitt, Unterabschnitt A. I. 1. a. aa.
[765] Siehe dazu ausführlich 3. Abschnitt, Unterabschnitt A. I. 1. b. aa.–cc.
[766] EGMR, *Loizidou v. Turkey* [GC], Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI.
[767] Vgl. auch *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties, S. 113.

Fallkonstellation der Entscheidung *Loizidou v. Turkey* unverkennbar wiedererkennen. Die nordzypriotischen Grundstücke sind Schutzobjekte, an denen die Beschwerdeführerin Eigentumsrechte hat. Der Gerichtshof hat hier richtigerweise erkannt, dass die örtliche Anwesenheit der Eigentümerin für eine Rechtsverletzung unerheblich ist. Immerhin hat gerade die Zugangsverweigerung die Verletzung des Rechts auf Eigentum aus Art. 1 des ersten Zusatzprotokolls der EMRK verursacht. Der Gerichtshof begründet allerdings die türkische Jurisdiktionsausübung nicht direkt mit der Kontrolle über die Grundstücke selbst. Vielmehr legt er ausführlich dar, dass die Türkei territoriale Gesamtkontrolle über Nordzypern ausübe. Die im nordzypriotischen Territorium befindlichen Grundstücke unterliegen dem Gerichtshof zufolge mithin auch der territorialen Gesamtkontrolle der Türkei. Damit ist das Konzept der Schutzobjektskontrolle zwar nicht vollumfänglich in dieser EGMR-Entscheidung niedergelegt. Denn die Schutzobjektskonzeption stellt gerade auf die direkte extraterritoriale Kontrolle von Schutzobjekten – unabhängig von einer territorialen Kontrolle – ab. Nichtsdestotrotz spricht die in dieser Entscheidung auffallend flexible Sichtweise des Gerichtshofs auch für den Grundgedanken der Schutzobjektstheorie. Der Fall unterscheidet sich nämlich durchaus von den typischen Fallgruppen der territorialen und personellen Kontrolle, die bislang die einzigen vom EGMR anerkannten Ausnahmefälle einer extraterritorialen Jurisdiktionsausübung sind.[768] Denn auch in den entschiedenen Fällen der Jurisdiktionsausübung aufgrund effektiver Territorialkontrolle befanden sich die betroffenen Individuen auf dem kontrollierten Gebiet. Nun könnte hier der Einwand erhoben werden, dass sich in der Spruchpraxis des EGMR zur Fragestellung der extraterritorialen Anwendbarkeit der Konvention nach der Entscheidung *Loizidou v. Turkey* – von *Banković* bis *Al-Skeini* – viel geändert hat.[769] Die Sichtweise des Gerichtshofs in dieser Entscheidung könnte folglich aufgrund der eigenen Spruchpraxis überholt sein. Allerdings wurde die Entscheidung *Loizidou* im Verlauf der gesamten einschlägigen Jurisprudenz stets zitiert.[770] Der EGMR hat von seiner *Loizidou*-Entscheidung nie Abstand genommen, geschweige denn ausdrücklich die Hauptaussagen dieser Entscheidung verworfen. Zwar verfolgt der EGMR einen restriktiven Ansatz hinsichtlich der extraterritorialen Anwendbarkeit der EMRK. Allerdings liefert die Spruchpraxis zugleich einen Ansatzpunkt für die Schutzobjektstheorie.

---

[768] So offenbar auch *Papp,* Extraterritoriale Schutzpflichten, S. 74, der den Fall *Loizidou v. Turkey* als eine gesonderte Fallgruppe der extraterritorialen Jurisdiktionsausübung einstuft und diese Gruppe mit dem Titel „extraterritoriale Sachen" versieht.

[769] Siehe oben 3. Abschnitt, Unterabschnitt A. I. 1. b. aa.–cc.

[770] Siehe beispielsweise EGMR, *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011, Rn. 133; *Issa and Others v. Turkey*, Rs. 31821/96, 16. November 2004, Rn. 68; *Al-Saadoon and Mufdhi v. the United Kingdom* (dec.), Rs. 61498/08, 30. Juni 2009, Rn. 127.

c. Schutzobjektskontrolle im Kontext der extraterritorialen Telekommunikationsüberwachung

Anhand der Schutzobjekts-Konzeption kann prinzipiell auch eine extraterritoriale Jurisdiktionsausübung in Fällen der grenzüberschreitenden Telekommunikationsüberwachung begründet werden. Das Konzept der Schutzobjektskontrolle erfasst grundsätzlich auch das Phänomen der Telekommunikationsüberwachung. Wie bereits ausgeführt, sind auch Telekommunikationsdaten, die unter den Schutz der Vertraulichkeit der Korrespondenz gemäß Art. 17 IPbpR und Art. 8 EMRK fallen, Schutzobjekte. Übt ein Staat in einem extraterritorialen Kontext Kontrolle über die Telekommunikationsdaten von Individuen aus, so kann dies die extraterritoriale Jurisdiktion des Staates aufgrund der Kontrolle über Schutzobjekte – in diesem Fall der Daten – begründen. Dabei unterscheidet sich die Art und Weise der Kontrolle in diesem Fall freilich von Fällen, in denen Kontrolle über körperliche Schutzobjekte ausgeübt wird. Neben diesem Aspekt werden im Folgenden außerdem Fallkonstellationen extraterritorialer Kontrolle über Telekommunikationsdaten aufgezeigt.

aa. Effektive „virtuelle" Kontrolle über Telekommunikationsdaten

Moderne Telekommunikationsüberwachung ist eine datenbasierte Form geheimdienstlicher Ausspähung. Denn die Spionage von Emails, Telefonaten oder Kurznachrichten ist letztlich eine Ausspähung der Telekommunikationsdaten, die als Datenpakete im globalen Telekommunikationsnetz unterwegs sind. Ein Staat kann über Daten freilich keine physische Kontrolle ausüben. Abgefangene Telekommunikationsdaten, die etwa in den Quartieren der Geheimdienste zur weiteren Analyse zwischengespeichert werden, befinden sich letztlich nicht in der physischen Kontrolle der Geheimdienste. Das schließt eine jurisdiktionsbegründende Kontrolle über Daten jedoch keineswegs von vornherein aus. Vielmehr muss das Konzept der „effektiven Kontrolle" zur Begründung extraterritorialer Jurisdiktionsausübung an die moderne Informations- und Telekommunikationstechnologie angepasst werden. So können Daten zwar nicht physisch kontrolliert werden, allerdings können sich Daten durchaus unter der virtuellen Kontrolle eines Geheimdienstes befinden. So kann ein Staat extraterritoriale Jurisdiktion über Daten ausüben, wenn sich diese unter seiner virtuellen Kontrolle befinden. Insofern ist der Literaturansicht, die für eine virtuelle Kontrolle über Daten zur Begründung extraterritoriale Jurisdiktion argumentiert[771], durchaus zuzustimmen. Dabei steht jedoch die Frage im Raum, wann ein Staat „virtuelle Kontrolle" über Daten ausübt.

Eine virtuelle Kontrolle über Daten ist dann anzunehmen, wenn sich die Daten im Einflussbereich des Staates befinden. Daten liegen wiederum dann im Einflussbereich des Staates, wenn sie ungehindert vom Staat ausgelesen, gespeichert oder auf andere Weise verarbeitet werden können, der Staat somit umfassenden Zugriff

[771] 3. Abschnitt, Unterabschnitt A. II. 3.

auf die Daten hat. Dafür ist indes nicht notwendig, dass sich der Datenträger oder die Datenkabel, durch welche die Daten fließen, selbst im Kontrollbereich des Staates befinden. Denn es ist technisch durchaus möglich und keineswegs unüblich, sich Fernzugriff auf diese Vorrichtungen zu verschaffen, ohne beispielsweise die Datenbank oder den Datenträger selbst zu kontrollieren. Des Weiteren kommt es auch nicht auf die Dauer an, in der die Daten im Einflussbereich des Staates sind. Auch durch kurze punktuelle Zugriffe auf Datenbanken befinden sich die betroffenen Daten im Einflussbereich und somit unter der virtuellen Kontrolle des Staates. Je kürzer die Dauer des Zugriffs ist, umso weniger Daten sind freilich betroffen.

Das Konzept der effektiven virtuellen Kontrolle über Daten widerspricht schließlich zumindest auch nicht der bisherigen Rechtsprechung des MRA. Freilich entspricht es nicht der engen Grundhaltung des EGMR und könnte allenfalls einen Ausnahmefall im Sinne des Regel-Ausnahme-Rechtsprechung des Gerichtshofs darstellen. Die Konzeption führt die Linie der bisher entwickelten Spruchpraxis zur extraterritorialen Jurisdiktionsausübung sachgemäß und modernisierend fort.[772] Letztlich lässt sich der Kerngedanke der virtuellen Kontrolle aus dem Fall der staatlichen Kontrolle über Individuen ableiten. In den anerkannten Fallgruppen effektiver Kontrolle über Individuen übt der Staat etwa durch die extraterritoriale Festnahme oder Folterung Gewalt über die Individuen aus. Das Individuum befindet sich für einen begrenzten Zeitraum im Einflussbereich des Staates und unterliegt damit der effektiven Kontrolle desselben. Die internationale Rechtsprechung nimmt hier zu Recht an, dass in solchen Fällen der Staat Jurisdiktion über das Individuum ausübt. Befürwortet man – wie dies vorliegend der Fall ist – die extraterritoriale Jurisdiktionsausübung aufgrund personeller Kontrolle durch gezielte Tötungen[773], so wäre dies ein Argument dafür, dass auch kurzzeitige und punktuelle Datenausspähungen eine virtuelle Kontrolle begründen können. Denn die durch die gezielte Tötungshandlung ausgeübte kurzzeitige Kontrolle über das Individuum wäre im Grundsatz mit der punktuellen Kontrolle der Daten vergleichbar. Demzufolge setzt eine extraterritoriale Jurisdiktionsausübung eine umfassende und ausschließliche Kontrolle über die Daten nicht voraus. Vielmehr kann auch eine effektive punktuelle Kontrolle hierfür ausreichen.[774] Insbesondere in Fällen der Telekommunikationsüberwachung werden nämlich häufig Konstellationen vorliegen, in denen kurzzeitige punktuelle Kontrolle durch die überwachenden Staaten ausgeübt wird.

[772] Siehe in diesem Zusammenhang 3. Abschnitt, Unterabschnitt A. I. 2.
[773] 3. Abschnitt, Unterabschnitt A. I. 2. b. bb. (2).
[774] *Margulies*, The NSA in Global Perspective, S. 11.

bb. Effektive „virtuelle" Kontrolle in einzelnen Überwachungskonstellationen

Im folgenden Unterabschnitt wird beleuchtet, inwieweit die Staaten in den einzelnen Konstellationen der Telekommunikationsüberwachung virtuelle Kontrolle über die Telekommunikationsdaten ausüben. Je nach Aufenthaltsort der betroffenen Individuen und dem Ort der Überwachungshandlung können sich unterschiedliche Fallkonstellationen ergeben.

So kann der Geheimdienst des Staates X etwa im Rahmen der Netzwerküberwachung mittels Datenkabelanzapfung die Telekommunikationsdaten eines Individuums, das sich im Staat Y befindet, anzapfen. Dabei kann heute aufgrund der weitreichenden technischen Handlungsmöglichkeiten der Geheimdienste auch die Lage des Anzapfpunktes – so etwa angezapfte Kabelleitungen oder Internetknotenpunkte – durchaus variabel sein. Der Geheimdienst des Staates X kann also theoretisch Datenkabel, die durch das eigene Staatsgebiet, durch das Staatsgebiet des Staates Y, durch ein Drittstaat Z oder auf dem Meeresboden laufen, anzapfen und den Datenfluss abfangen (Abbildung 1).

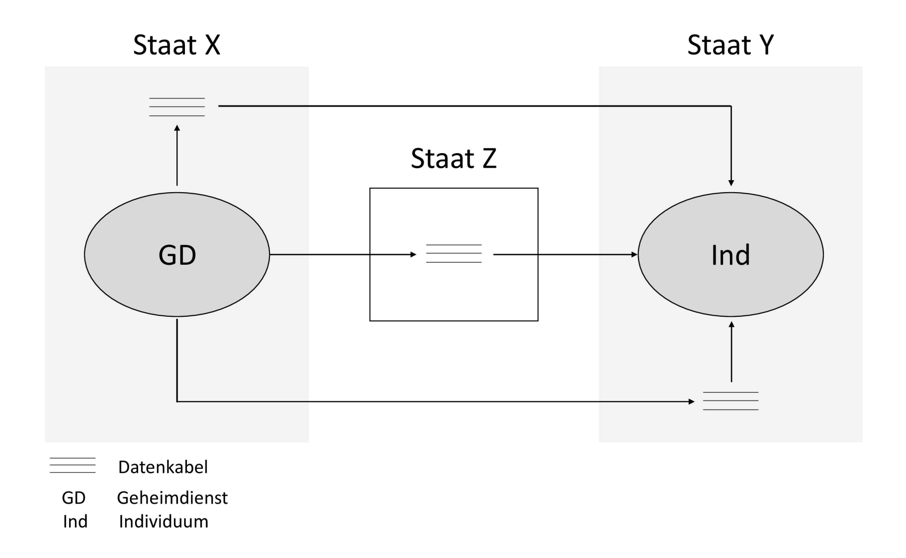


Abbildung 1: Konstellationen des extraterritorialen Zugriffs auf das Telekommunikationsnetzwerk

Ähnliche Konstellationen sind auch hinsichtlich der Beschaffung von Daten mithilfe von *Service Providern* möglich. So kann der Geheimdienst sowohl aus Servern von S*ervice Provider*, die sich im Inland befinden, Daten über das im Staat Y ansässigen Individuum entnehmen. Gleichermaßen ist eine Datenentnahme aus Servern, die sich etwa im Staat X oder dem Drittstaat Z befinden, denkbar (Abbildung 2).

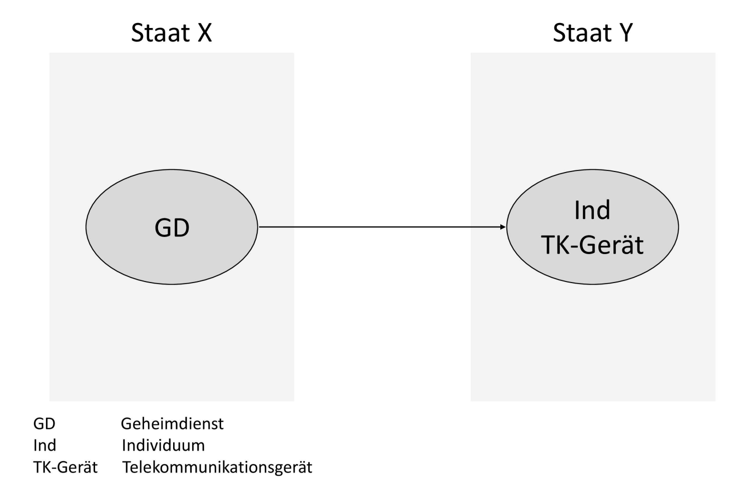


Abbildung 2: Konstellationen der extraterritorialen Beschaffung von Telekommunikationsdaten aus Servern von Service Providern

Im Regelfall befinden sich private Telekommunikationsgeräte – wie etwa Mobiltelefone oder Laptops – bei den Eigentümern oder Besitzern. Hinsichtlich der Überwachung dieser Geräte kann davon ausgegangen werden, dass diese örtlich nicht vom Individuum getrennt sind. Insofern wird in extraterritorialen Konstellationen dieser Überwachungsform der Geheimdienst des Staates X das Gerät des Individuums im Staat Y ausspähen (Abbildung 3).

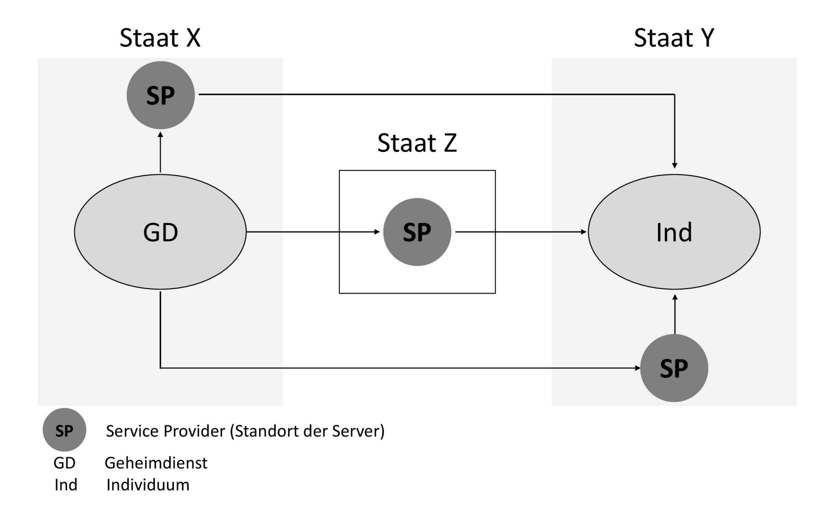


Abbildung 3: Konstellationen des extraterritorialen Zugriffs auf private Telekommunikationsgeräte

(1) Zugriff auf das Telekommunikationsnetzwerk

Geheimdienste können nur mithilfe technischer Vorrichtungen direkten Zugriff zum Datenverkehr des internationalen Telekommunikationsnetzwerks gewinnen. Dabei stehen zweifelsfrei unterschiedliche Technologien zur Verfügung, von denen wahrscheinlich viele noch geheim sind. Ab wann und inwieweit Geheimdienste virtuelle Kontrolle über die im globalen Telekommunikationsnetz fließenden Daten ausüben, müsste strenggenommen anhand einer präzisen Untersuchung der eingesetzten Überwachungstechnik im konkreten Einzelfall beantwortet werden. Die Geheimheit der konkreten Vorgehensweisen erlaubt solch einen gründlichen Blick an dieser Stelle nicht. Jedoch kann auch ohne Kenntnis über die Details der konkreten Überwachungstechnologie durchaus die aufgeworfene Frage nach der virtuellen Kontrolle über die Telekommunikationsdaten beantwortet werden. Denn jedenfalls ermöglicht die Installation der Überwachungstechnik – unabhängig von ihrer konkreten Funktionsweise – im Ergebnis den Zugriff und einen umfassenden Einblick auf den durchfließenden Datenverkehr. Beispielhaft wurde oben der Einsatz von Kabelteilern (*splitter*), die an Untersee-Glasfaserkabel angebracht werden, sowie von IMSI-Catchern dargestellt.[775] Solche Zugriffe auf das Telekommunikationsnetzwerk ermöglichen einerseits eine Echtzeit-Abhörung des durchfließenden Datenverkehrs auf dem Übertragungsweg vom Absender zum Empfänger. Des Weiteren wird das Kopieren und Abspeichern der Daten auf eigene Datenträger ermöglicht. Somit befinden sich alle Daten, die durch die angezapfte Stelle des Teekommunikationsnetzwerks fließen, ab dem Moment, in dem der Anzapf-Prozess beginnt, im Einflussbereich des Geheimdienstes. Gleichzeitig fließen sie im Netzwerk weiter. Die abgefangenen Daten befinden sich somit unter der virtuellen Kontrolle des agierenden Geheimdienstes. Dabei übt der Geheimdienst jedoch in der Regel keine Kontrolle über die gesamte Telekommunikationsinfrastruktur aus.[776] Dies ist auch für das Vorliegen virtueller Kontrolle keineswegs zwingend.[777] Für eine extraterritoriale Jurisdiktionsausübung kann es genügen, dass der Staat nur über die Telekommunikationsdaten Kontrolle ausübt. So ist auch unstreitig anerkannt, dass die Kontrolle über ein Individuum die Jurisdiktion des Staates begründen kann, ohne dass es einer Kontrolle über das Gebiet, auf dem sich das Individuum befindet, bedarf. Gleiches muss sinngemäß auch für den Fall der virtuellen Kontrolle

---

[775] Siehe 1. Abschnitt, Unterabschnitt B. III. 2. a.

[776] Anderer Ansicht ist offenbar das UN-Hochkommissariat für Menschenrechte (OHCHR), das in seinem einschlägigen Bericht hierzu folgendermaßen Stellung nimmt: „It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant.", Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/27/37, 30. Juni 2014, Rn. 34.

[777] Vgl auch *Seibert-Fohr,* Digital Surveillance, Meta Data and Foreign Intelligence Cooperation, S. 10.

über Daten gelten.[778] Zudem wurde bereits aufgezeigt, dass eine kurzzeitige punktuelle Kontrolle über die Daten ausreicht. Dies ist im Rahmen dieser Fallgruppe für Echtzeit-Überwachungen relevant, bei denen die erfassten Telekommunikationsdaten sofort analysiert und wegen Unbrauchbarkeit direkt gelöscht werden. Hierbei würden sich die Daten nur für einen kurzen Zeitraum im Einflussbereich des Geheimdienstes befinden. Dies würde indes für eine Jurisdiktionsbegründung genügen.[779]

(2) Beschaffung von Telekommunikationsdaten aus Servern von *Service Providern*

Im Zuge der Inanspruchnahme von Internet- und Kommunikationsdienstleistungen ist es unumgänglich, dass sich die Benutzerdaten der Dienstleistungsnutzer sowie die Verkehrs- und Inhaltsdaten der durchgeführten Dienstleistungen (wie etwa Emailverkehr) selbst zumindest zeitweise auf den Servern der *Service Provider* befinden. Für die einwandfreie Abwicklung internetbasierter Dienstleistungen ist eine Speicherung der Daten erforderlich. Im Rahmen von obligatorischen Vorratsdatenspeicherungen sind die *Service Provider* per Gesetz zur Speicherung verpflichtet. All diese auf den Servern gespeicherten Daten befinden sich im Einflussbereich der *Service Provider*. Im Rahmen einer regulären Durchführung der Dienstleistungen verfügen grundsätzlich auch nur die *Service Provider*, die von den Nutzern zur Abwicklung der Dienste beauftragt wurden, über umfassenden Zugriff auf diese Daten. Im Rahmen geheimdienstlicher Überwachungsprogramme wird die ausschließliche Einflussnahme der Internetdienstleister indes durchbrochen. So dringen die Geheimdienste im Zuge ihrer Überwachungsmaßnahmen in diesen Einflussbereich ein.

Verschafft sich ein Geheimdienst unbefugt geheimen Zugriff auf die Server der *Service Provider*, so kann er die abgespeicherten Daten einsehen und diese für eigene Zwecke verwenden. Die Daten befinden sich in solch einem Fall somit auch im Einflussbereich des Geheimdienstes, der damit virtuelle Kontrolle über diese Daten ausübt. Dass sich die Daten dabei nicht ausschließlich im Einflussbereich des Geheimdienstes, sondern daneben auch weiterhin im Einflussbereich des *Service Providers* befinden, spielt keine Rolle. Ohne dass der *Service Provider* in diesem Fall davon Kenntnis hat oder im Vorfeld zugestimmt hätte, teilt er sich letztlich die Kontrolle über die Daten mit dem Geheimdienst.[780] Diese Konstellation ist indes vergleichbar mit Fällen der territorialen Kontrolle, in denen ein Besatzungsstaat nur partielle

[778] Siehe dazu auch *Margulies,* The NSA in Global Perspective, S. 11, der mit der Entscheidung des EGMR im Fall *Öcalan v. Turkey* [GC], Rs. 46221/99, 12. Mai 2005, Rep. 2005-IV argumentiert: „In *Ocalan*, Turkish officials in Kenya had jurisdiction over the suspect [...], even though Kenya clearly retained jurisdiction over its own territory [...]. If this is true, jurisdiction may be divisible [...]: jurisdiction over electronic communications may as a *de facto* matter be shared between countries, even when only one of those states has jurisdiction over territory and persons."

[779] Siehe bereits oben 3. Abschnitt, Unterabschnitt A. II. 4. c. aa.

[780] Zur grundsätzlichen Teilbarkeit jurisdiktionsbegründender effektiver Kontrolle in extraterritorialen Zusammenhängen siehe *Margulies,* The NSA in Global Perspective, S. 11.

Kontrolle über das Gebiet des besetzten Staates ausübt und damit die Kontrolle über das Territorium zwischen beiden Staaten aufgeteilt ist. Dies steht indes einer jurisdiktionsbegründenden effektiven Kontrolle nicht entgegen. Gleiches muss auch für den dargestellten Fall des heimlichen Zugriffs auf Server von *Service Provider* gelten.

Das gleiche gilt im Ergebnis auch für Fälle, in denen ein Geheimdienst mit Zustimmung und Kenntnis des *Service Providers* Zugriff auf die Daten im Server hat. Hierbei übt er gleichermaßen virtuelle Kontrolle über die Daten aus. Der einzige Unterschied besteht darin, dass hierbei der *Service Provider* den Zugriff zulässt. Dieser Umstand wirkt sich allerdings auf die Ausübung virtueller Kontrolle durch den Geheimdienst nicht aus. Demzufolge üben Geheimdienste in Fällen des Direktzugriffs auf Servern von *Service Providern* virtuelle Kontrolle über die gespeicherten Daten aus, unabhängig davon, ob der Zugriff geheim und unbefugt oder mit Zustimmung des Internetdienstleisters erfolgt.

Neben diesen Varianten der Überwachung, in denen der Geheimdienst direkten Zugriff auf die Server der Internetdienstleister hat, kann ein *Service Provider* auch nur ausgewählte Daten dem Geheimdienst zur Verfügung stellen. Dies kann auf Grundlage einer rechtlichen Verpflichtung oder auf freiwilliger Kooperation basieren. Der Geheimdienst kann dabei nur die zur Verfügung gestellten Daten einsehen und verarbeiten und übt demnach nur über diese Daten virtuelle Kontrolle aus. Der Kontrollradius ist in diesem Fall mithin geringer, da der Geheimdienst nicht mehr den gigantischen Datenpool der Server nutzen kann, sondern vielmehr auf die Auswahl der zur Verfügung gestellten Daten beschränkt ist. Dies ändert jedoch nichts an der Qualität der ausgeübten Kontrolle – jedenfalls übt der Geheimdienst effektive virtuelle Kontrolle über diese Datenauswahl aus.

(3) Zugriff auf private Telekommunikationsgeräte

Hackt sich ein Geheimdienst in privatgenutzte Telekommunikationsgeräte ein, so gewinnt er umfassenden Zugriff auf alle verfügbaren Daten, die sich auf dem Gerät – beispielsweise auf dem infizierten Laptop – befinden. So können die Daten weitgehend problemlos vom Geheimdienst kopiert und abgespeichert werden. Außerdem können Korrespondenz sogar in Echtzeit abgehört werden. Hier liegt es auf der Hand, dass sich die auf dem Zielgerät abgespeicherten Daten infolge dieser intensiven Form der Überwachung im Einflussbereich des Geheimdienstes befinden. Gewöhnlich befinden sich Geräte wie PCs oder Smartphones samt den abgespeicherten Daten im ausschließlichen Macht- und Kontrollbereich der nutzenden Individuen. Der geheimdienstliche Übergriff behindert die Individuen letztlich auch nicht an der Verwendung der Geräte. Vielmehr läuft der geheimdienstliche Überwachungsprozess im Hintergrund, ohne dass das Individuum dies überhaupt bemerkt. Durch den Übergriff gewinnt jedoch der Geheimdienst neben den berechtigten Individuen umfassende virtuelle Kontrolle über die Daten.

cc. Rechtsfolgenseite: Reichweite der extraterritorialen Pflichten

Infolge der Jurisdiktionsausübung des Drittstaates über die Telekommunikationsdaten ist er grundsätzlich zur Achtung der Menschenrechte aus dem IPbpR und der EMRK verpflichtet. Allerdings stellt sich die Frage nach der Reichweite der Verpflichtung des Drittstaates. Der Drittstaat könnte wie in Fällen der umfassenden territorialen Kontrolle vollumfänglich zur Umsetzung aller in den Menschenrechtspakten kodifizierten Rechte verpflichtet sein.[781] Möglich wäre indes auch eine am Maß seiner Kontrollausübung begrenzte Menschenrechtsverpflichtung. Letzteres ist bislang in Fällen der punktuellen Kontrolle über Individuen anerkannt.[782]

Der Fall der Jurisdiktionsausübung über Telekommunikationsdaten ist jedoch strenggenommen mit diesen beiden Fallgruppen nicht vergleichbar. Denn der Drittstaat kontrolliert einerseits keine Individuen, sondern übt extraterritoriale Jurisdiktion über Daten aus. Die Kontrolle kann dabei entweder in Fällen von gezielten Einzelüberwachungen Datenpakete einzelner Telekommunikationen betreffen. Im Rahmen von Massenüberwachungsmaßnahmen erstreckt sich die jurisdiktionsbegründende virtuelle Kontrolle indes auf ein enorm hohes Datenvolumen. Gerade im letzten Fall erscheint ein Vergleich mit der Ausübung extraterritorialer Kontrolle über einzelne Individuen fernliegend zu sein. So kann das Ausmaß der Telekommunikationskontrolle erheblich weitreichender sein als die punktuelle Kontrolle über einzelne Individuen.

Mit militärischen Besatzungsfällen und anderen Formen der umfassenden Gebietskontrolle ist die Fallgruppe der Telekommunikationsüberwachung indes auch nicht gleichzusetzen. Zwar ist durch diese Form der geheimdienstlichen Überwachung das Telekommunikationsnetzwerk des Aufenthaltsstaates betroffen, das zweifelsfrei in der heutigen Welt eine komplexe und für den Staat bedeutsame Infrastruktur darstellt. Dennoch kontrolliert der Drittstaat nicht flächendeckend institutionelle Strukturen, die das politische Fundament des Aufenthaltsstaates bilden. Dies ist letztlich ein wesentlicher Unterschied zum Fall der umfassenden extraterritorialen Kontrolle über ein fremdes Territorium. Dies spricht letztlich auch gegen eine vollumfängliche Verpflichtung des Drittstaates gegenüber den betroffenen Individuen. Denn trotz der möglichen Kontrolle über ein sehr großes Datenvolumen bleibt die staatliche Jurisdiktionsausübung auf einen spezifischen Bereich – nämlich der Telekommunikation von Individuen innerhalb des Aufenthaltsstaates – begrenzt. Überzeugender ist aus diesem Grund die Begrenzung der menschenrechtlichen Verpflichtung des Drittstaates auf das Maß seiner Kontrollausübung. So wäre der Drittstaat demnach gegenüber den betroffenen Individuen zur Umsetzung der Menschenrechte verpflichtet, die durch die extraterritorialen Überwachungsmaßnahmen tangiert werden. Insbesondere wären etwa die aus dem Recht der Privatsphäre gemäß Art. 17 IPbpR und Art. 8 EMRK hervorgehenden Pflichten betroffen. Der Drittstaat müsste etwa die aus dem Schutz der Vertraulichkeit der

---

[781] Siehe oben 3. Abschnitt, Unterabschnitt A. I. 3. a.

[782] 3. Abschnitt, Unterabschnitt A. I. 3. b.

Korrespondenz und der personenbezogenen Daten fließenden Grundsätze beachten und ist für jegliche Verletzungen seiner Pflichten aus diesen Menschenrechten gegenüber den betroffenen Individuen verantwortlich.

5. Ergebnis

Die Schutzobjektstheorie erfasst somit Fälle der extraterritorialen Jurisdiktionsausübung, die nicht auf territorialer oder personeller Kontrolle beruhen, sondern vielmehr aufgrund der Kontrolle über menschenrechtlich relevante Schutzobjekte entstehen. Diese Konzeption fügt sich in die Reihe der bisher in der Literatur entwickelten Ansätze zum Problem der extraterritorialen Anwendbarkeit der internationalen Menschenrechtspakte in Fällen der modernen geheimdienstlichen Überwachung der globalen Telekommunikation ein. Auf Grundlage dieses Konzeptes kann die extraterritoriale Anwendbarkeit des IPbpR und der EMRK in Fällen der grenzüberschreitenden Telekommunikationsüberwachung – und daneben auch in Fällen der extraterritorialen Kontrolle über andere Schutzobjekte – dogmatisch fundiert begründet werden. Damit können Drittstaaten, die durch grenzüberschreitende Durchführungen von Überwachungsmaßnahmen die Korrespondenzen von Individuen im Aufenthaltsstaat ausspähen, ihre Menschenrechtsverpflichtungen aus den Art. 17 IPbpR und Art. 8 EMRK verletzen. Sie sind dabei an den aus diesen Artikeln hervorgehenden menschenrechtlichen Pflichten und Prinzipien – wie sie im 2. Abschnitt der vorliegenden Arbeit eingehend dargestellt wurden – gegenüber den betroffenen Individuen im Aufenthaltsstaat gebunden.

B. Verletzung des Schutzes der Privatsphäre durch den Aufenthaltsstaat

In grenzüberschreitenden Überwachungskonstellationen kann neben der Überwachungshandlung des Drittstaates auch das Handeln oder Unterlassen des Aufenthaltsstaates in bestimmten Fallsituationen einen Eingriff in den Schutz der Vertraulichkeit der Korrespondenz und der personenbezogenen Daten gemäß Art. 17 IPbpR und Art. 8 EMRK darstellen. So kommen je nach Art der Beteiligung oder des Unterlassens eine Verletzung von menschenrechtlichen Schutzpflichten durch den Aufenthaltsstaat oder eine Beihilfe zur Menschenrechtverletzung des Drittstaates in Betracht. Außerdem wirft das Phänomen *Intelligence Sharing*, d.h. der zwischenstaatliche Austausch von ausgespähten Telekommunikationsdaten, Fragen der menschenrechtlichen Verantwortlichkeit des beteiligten Dritt- und Aufenthaltsstaates auf.

I. Verletzung von menschenrechtlichen Schutzpflichten

1. Die Schutzpflichtdogmatik im internationalen Menschenrechtsschutz: Grundlagen, Voraussetzungen und Grenzen der Schutzpflichten

Während die Staaten aus den menschenrechtlichen Abwehrrechten zum Unterlassen von Eingriffshandlungen verpflichtet werden, sind sie aus den Schutzpflichten wiederum zur Ausübung von geeigneten faktischen oder rechtlichen Handlungsmaßnahmen zum Schutz individueller Rechte verpflichtet.[783] In der internationalen Spruchpraxis – insbesondere aber in der Judikatur des EGMR – findet in diesem Zusammenhang indes der weite Begriff „*positive obligations*" (positive Verpflichtungen) Verwendung.[784] Dabei handelt es sich um einen in Abgrenzung zu den negativen Verpflichtungen (Abwehrrechte) entwickelten Oberbegriff, der alle auf positives Tun der Staaten gerichteten Verpflichtungen umfasst.[785] Schutzpflichten bilden eine Untergruppe der positiven Verpflichtungen. Weiterhin werden beispielsweise auch Leistungsrechte, verfahrensrechtliche und institutionelle Garantien unter die „*positive obligations*" gefasst.[786]

Es ist heute allgemein im Bereich des internationalen Menschenrechtsschutzes anerkannt, dass die Staaten nicht nur zum Unterlassen von Eingriffshandlungen verpflichtet sind, sondern auch zum aktiven Schutz vor Menschenrechtsverletzungen verpflichtet sein können.[787] Wenn etwa die Verletzungshandlung nicht vom Staat selbst ausgeht, sondern durch Dritte ausgelöst wird, kann der Staat durch bloßes Unterlassen keinen effektiven Schutz der bedrohten Menschenrechte bewirken. Als Verursacher der Menschenrechtsverletzungen kommen dabei beispielsweise

[783] *Stahl,* Schutzpflichten im Völkerrecht, S. 35; *Akandji-Kombe*, Positive obligations under the European Convention on Human Rights, S. 7.

[784] Siehe etwa EGMR, *Marckx v. Belgium*, Rs. 6833/74, 13. Juni 1979, Serie A31. Der MRA verwendet den Begriff beispielsweise im UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004; siehe außerdem *Annakkarage Suranjini Sadamali Pathmini Peiris v. Sri Lanka*, No. 1862/2009, CCPR/C/103/D/1862/2009, 18. April 2012.

[785] *Stahl,* Schutzpflichten im Völkerrecht, S. 37.

[786] *Dröge,* Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 5; *Nowak*, CCPR Commentary, S. XXI, Rn. 4. Für eine ausführliche Bestimmung des Begriffs „Schutzpflicht" sowie der Abgrenzung von den anderen Formen positiver Handlungspflichten (wie etwa Leistungsrechte oder verfahrensrechtliche Garantien) siehe *Stahl,* Schutzpflichten im Völkerrecht, S. 35 ff.

[787] Siehe *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 118 f.

Privatpersonen[788], ausländische Staatsorgane[789] oder auch Naturkatastrophen[790] in Betracht. Der EGMR hat bereits sehr früh in seiner Rechtsprechung anerkannt, dass positive Verpflichtungen – und damit auch Schutzpflichten im engeren Sinne – in der EMRK verankert sind.[791] Auch der Menschenrechtsausschuss hat in seiner Spruchpraxis bestätigt, dass die im IPbpR niedergelegten Menschenrechte neben den negativen Pflichten auch positive Verpflichtungen beinhalten.[792] So sind in den Menschenrechtspakten einerseits allgemeine Gewährleistungsgarantien vorhanden, wie etwa in Art. 1 EMRK sowie Art. 2 Abs. 2 lit. a IPbpR.[793] Außerdem sind Schutzpflichten auch ausdrücklich in einzelnen Menschenrechtsnormen niedergelegt, so etwa in Art. 17 IPbpR und in Art. 6 Abs. 1 S. 2 IPbpR sowie in Art. 2 Abs. 1 EMRK.[794]

Darüber hinaus leiten der EGMR und der Menschenrechtsausschuss für die anderen Menschenrechte Schutzpflichten grundsätzlich aus den allgemeinen Gewährleistungsgarantien in Art. 1 EMRK bzw. Art. 2 IPbpR in Verbindung mit den materiellen Rechten ab.[795]

Die Staaten sind aus den menschenrechtlichen Schutzpflichten zum Handeln verpflichtet, wenn eine Reihe von Voraussetzungen erfüllt sind. So darf einerseits kein staatlicher Eingriff in das Recht der Individuen vorliegen, da in diesem Fall der

---

[788] EGMR, *Airey v. Ireland,* Rs. 6289/73, 09. Oktober 1979, Serie A 32. UN Human Rights Committee, *Annakkarage Suranjini Sadamali Pathmini Peiris v. Sri Lanka*, No. 1862/2009, CCPR/C/103/D/1862/2009, 18. April 2012, Rn. 7.2.

[789] Siehe etwa EGMR, *Ilaşcu and Others v. Moldova and Russia* [GC]*,* Rs. 48787/99, 8. Juli 2004, Rep. 2004-VII, Rn. 333; außerdem *El-Masri v. The former Yugoslav Republic of Macedonia*, Rs. 39630/09, 13.12.2012, Rep. 2012, Rn. 206.

[790] So etwa in EGMR, *Budayeva and Others v Russia,* Rs. 15339/02, 11673/02, 15343/02, 20058/02, 21166/02, 20. März 2008, Rep. 2008 sowie *Öneryildiz v. Turkey* [GC], Rs. 48939/99, 30. November 2004, Rep. 2004-XII.

[791] Siehe statt vieler EGMR, *Marckx v. Belgium*, Rs. 6833/74, 13. Juni 1979, Serie A31, Rn. 31.

[792] *Nowak*, CCPR Commentary, S. XXI, Rn. 4. Vgl dazu etwa *William Eduardo Delgado Páez v. Colombia*, No. 195/1985, CCPR/C/39/D/195/1985, 12. Juli 1990, Rn. 5.5; UN Human Rights Committee, General Comment No. 31 (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), CCPR/C/21/Rev.1/Add. 13, 26. Mai 2004, Rn. 8.

[793] Auch in anderen Menschenrechtspakten sind solche Gewährleistungsgarantien zu finden: Art. 1 AMRK, Art. 1 AfCRMV, Art. 2 Abs. 2 IPwskR.

[794] *Stahl* verweist zudem auf ausdrückliche Schutzbestimmungen in den Schrankenregelungen einzelner Menschenrechte wie in Art. 8 Abs. 2 EMRK oder Art. 9 Abs. 2 EMRK. Siehe *Stahl,* Schutzpflichten im Völkerrecht, S. 104.

[795] Siehe etwa UN Human Rights Committee, *S. S. v. Norway,* No. 79/1980, CCPR/C/15/D/79/1980, 2. April 1982, Rn. 4.2, außerdem *Stahl,* Schutzpflichten im Völkerrecht, S. 113. Für die Spruchpraxis des EGMR siehe *McCann and Others v. Vereinigtes Königreich,* Rs. 18984/91, 27. September 1995, Serie A 324, Rn. 161 sowie *Ress,* The Duty to Protect and to Ensure Human Rights under the European Convention on Human Rights, in Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights, S.183; *Akandji-Kombe*, Positive obligations under the European Convention on Human Rights, S. 8; *Stahl,* Schutzpflichten im Völkerrecht, S. 109 f. Die Autoren weisen darauf hin, dass der EGMR in älteren Entscheidungen Schutzpflichten allein aus den materiellen Rechten abgeleitet hat, bevor er zu einer kombinierten Ableitung aus der allgemeinen Gewährleistungsgarantie in Verbindung mit den materiellen Rechten übergegangen ist.

Staat auf Grundlage der Abwehrrechte zum Unterlassen verpflichtet wäre.[796] Stattdessen muss ein sogenannter „Übergriff“ von dritter Seite vorliegen, der eine Beeinträchtigung der Menschenrechte zur Folge hat.[797] Aufgrund des Übergriffs muss somit das Individuum in der Ausübung seiner Rechte verhindert oder zumindest gestört werden, wobei die Gefährdung der Rechtsausübung genügen kann.[798] Allein durch das Vorliegen eines solchen Übergriffs verletzt ein Staat indes noch nicht Schutzpflichten. Für eine Schutzpflichtverletzung kommt es vielmehr darauf an, ob der Staat in Kenntnis des Übergriffs und der (zumindest drohenden) Rechtsbeeinträchtigung geeignete Schutzmaßnahmen unterlassen hat.[799] Dabei muss zwischen der Nichtvornahme von Schutzmaßnahmen durch den Staat und der Rechtsgefährdung oder -beeinträchtigung ein Kausalzusammenhang bestehen.[800]

Ist ein Staat nach den Menschenrechtspakten schutzverpflichtet, so kommen regelmäßig unterschiedliche Schutzmaßnahmen zur Ausführung in Betracht. Dabei verfügen die Staaten über einen weiten Ermessenspielraum hinsichtlich der Auswahl der Maßnahmen.[801] Innerhalb des Ermessensrahmens müssen die Staaten in Abwägung ihrer eigenen Interessen und dem Schutzinteresse des Individuums eine angemessene Maßnahme wählen.[802] Schutzpflichten können in Fällen der proaktiven Gefahrenbeseitigung *präventiv* oder aber in Fällen der Beseitigung von eingetretenen Rechtsbeeinträchtigungen *kurativ*[803] sein.[804] Zu den kurativen Maßnahmen gehören auch Restitutions- und Kompensationsmaßnahmen.[805] Außerdem können die Staaten zwischen faktischen Schritten oder rechtlichen und gesetzgeberischen Maßnahmen wählen. Ihr Ermessenspielraum kann jedoch aufgrund der gegebenen

[796] *Stahl,* Schutzpflichten im Völkerrecht, S. 122; *Dröge* verwendet hier den weiteren Begriff „Beeinträchtigung“, siehe dazu *Dröge*, Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 346 f.

[797] Ausführlich zum schutzrechtlichen „Übergriff“: *Stahl,* Schutzpflichten im Völkerrecht, S. 137 ff.

[798] Ebd., S. 150.

[799] *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 125.

[800] *Ress,* The Duty to Protect and to Ensure Human Rights under the European Convention on Human Rights, in Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights, S. 181. EGMR, *Botta v. Italy,* Rs. 21439/93, 24. Februar 1998, Rep. 1998-I, Rn. 34; EKMR, *Tugar v. Italy,* Rs. 22869/93, 18. Oktober 1995, D.R.83-A, S. 26. Eine abweichende Sichtweise vertritt *Stoyanova,* Human Trafficking and Slavery Reconsidered, der die Formulierung „*proximity test*“ verwendet: „Thus, there is no requirement for causality. Yet there needs to be proximity between the harm and the state omission“ (S. 328).

[801] EGMR, *Plattform „Ärzte für das Leben“ v. Austria*, Rs. 10126/82, 21. Juni 1988, Serie A139; *Fadeyeva v. Russia,* Rs. 55723/00, 09. Juni 2005, Rep. 2005-IV, Rn. 96: „Where the State is required to take positive measures, the choice of means is in principle a matter that falls within the Contracting State’s margin of appreciation“.

[802] So etwa der EGMR in *Fadeyeva v. Russia,* Rs. 55723/00, 09. Juni 2005, Rep. 2005-IV, Rn. 134: „it has failed to strike a fair balance between the interests of the community and the applicant’s effective enjoyment of her right to respect for her home and her private life“.

[803] Stahl verwendet hier den Begriff „repressiv“, *Stahl,* Schutzpflichten im Völkerrecht, S. 328.

[804] *Kälin/Künzli,* Universeller Menschenrechtsschutz, S. 123.

[805] *Ress,* The Duty to Protect and to Ensure Human Rights under the European Convention on Human Rights, in Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights, S. 196 ff.

Umstände begrenzt sein. So sind die Staaten grundsätzlich dazu verpflichtet, mithilfe geeigneter und angemessener Mittel einen Mindestschutz zu gewährleisten.[806] Andererseits enden ihre Schutzverpflichtungen an einer Obergrenze, die sich letztlich aus den Umständen des konkreten Sachverhalts ergibt. So müssen die Staaten zwar geeignete Schutzmaßnahmen vornehmen, allerdings obliegt ihnen keine absolute Verhinderungspflicht von Menschenrechtsbeeinträchtigungen:[807]

> „Whether or not the authorities' efforts could in principle have averted the fatal outcome in the present case is not decisive for this conclusion. What matters for the Court is whether they did everything reasonably possible in the circumstances, in good faith and in a timely manner, to try to save the first applicant's life".[808]

Auch Umstände wie rechtliche und faktische Unmöglichkeit können das Pflichtmaß des Staates begrenzen.[809] Letztendlich entscheiden die konkreten Faktoren des Einzelfalls – wie etwa die Schwere der Rechtsbeeinträchtigung oder die besondere Schutzbedürftigkeit des betroffenen Individuums – über die Reichweite des staatlichen Schutzpflichtumfangs.[810]

Der EGMR und der MRA gehen auch in Hinblick auf die Schutzpflicht-Dogmatik kasuistisch vor. Letztlich haben sie die Grundprinzipien und Voraussetzungen der menschenrechtlichen Schutzpflichten anhand der zu beurteilenden Einzelfälle entwickelt. So hängen die Reichweite und die Grenzen der Schutzpflichten von den Umständen des Einzelfalles ab. Im folgenden Unterkapitel werden anhand des konkreten Falles der grenzüberschreitenden Telekommunikationsüberwachung die einzelnen Voraussetzungen und Prinzipien der Schutzpflichten vertieft.

2. Schutzpflichten aufgrund von extraterritorialen Übergriffen eines Drittstaats?

In extraterritorialen Fallkonstellationen können neben den abwehrrechtlichen Menschenrechtsverpflichtungen auch Schutzpflichten der involvierten Staaten relevant werden. Dabei sind insbesondere zwei Grundkonstellationen denkbar. Entweder steht die Frage nach extraterritorialen Schutzpflichten im Raum, also der Verpflichtung eines Staates Menschenrechte von Individuen im Ausland zu schützen.[811] Des Weiteren kann die Schutzverpflichtung eines Staates relevant sein, auf dessen Territorium Menschenrechtseingriffe durch Drittstaaten vorgenommen werden. Letztere Variante entspricht dem zugrundeliegenden Untersuchungsgegenstand der

[806] *Stahl,* Schutzpflichten im Völkerrecht, S. 330 f.
[807] Ebd., S. 317 f.
[808] EGMR, *Salakhov and Islyamova v. Ukraine,* Rs. 28005/08, 14. März 2013, Rn. 181.
[809] *Stahl,* Schutzpflichten im Völkerrecht, S. 321 ff.
[810] Vgl. *Dröge*, Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 335. Nach Dröge verdichte sich das Maß der Schutzverpflichtung des Staates, je weniger das Individuum der Grundrechtsbeeinträchtigung aus eigener freier Entscheidung entgehen könne.
[811] Zu dieser Fallkonstellation siehe *Papp,* Extraterritoriale Schutzpflichten.

extraterritorialen Telekommunikationsüberwachung. Zu prüfen wäre dabei, ob und inwieweit der Aufenthaltsstaat aufgrund der vom Drittstaat ausgeübten extraterritorialen Korrespondenzüberwachung zum Schutz betroffener Individuen verpflichtet ist. Dass grundsätzlich auch Akte von Drittstaaten schutzpflichtenbegründende Übergriffe sein können, wurde bereits im vorangegangenen Unterabschnitt kurz erwähnt.[812] Die extraterritorialen Akte eines Staates, die Menschenrechte von Individuen innerhalb des Territoriums eines anderen Staates tangieren, können prinzipiell durchaus Schutzpflichten des Aufenthaltsstaates begründen. Allerdings stellt sich die Frage, inwieweit dies auch für Fälle gilt, in denen der Drittstaat aufgrund der konkreten Gesamtumstände extraterritoriale Jurisdiktion entweder über das fremde Gebiet, über einzelne Individuen oder über konkrete Schutzobjekte[813] ausübt. Die Jurisdiktion des Drittstaates aufgrund der Ausübung effektiver Kontrolle bedeutet auf der anderen Seite nämlich zumindest eine Reduzierung der faktischen Gewaltausübung des Aufenthaltsstaates über das betroffene Gebiet, die betroffenen Individuen oder Schutzobjekte. Insofern kann im Einzelfall fraglich sein, inwieweit der schutzverpflichtete Aufenthaltsstaat faktisch Maßnahmen ergreifen kann.

Im Fall der extraterritorialen Telekommunikationsausübung können – nach hier vertretener Ansicht – die Drittstaaten aufgrund effektiver Kontrolle über die Telekommunikationsdaten betroffener Individuen extraterritoriale Jurisdiktion über diese Schutzobjekte ausüben. Die effektive virtuelle Kontrolle über die Telekommunikationsdaten schließt den Aufenthaltsstaat jedoch keineswegs dauerhaft davon aus, Kontrolle über diese Schutzobjekte auszuüben. Zwar befinden sich die Daten im Moment der Überwachungshandlung tatsächlich – sei es auch nur für einen kurzen Moment – unter der virtuellen Kontrolle des Drittstaates.[814] Allerdings ist der Aufenthaltsstaat vor, während oder nach der Durchführung der geheimdienstlichen Überwachungshandlungen keineswegs von seiner Jurisdiktionsausübung über diese Schutzobjekte per se ausgeschlossen. Letztlich sind hier die konkreten Umstände der Überwachungsmethodik entscheidend. In der Regel ist der Aufenthaltsstaat jedenfalls durchaus in der Lage, geeignete Schutzmaßnahmen umzusetzen. Allerdings ist seine Schutzverpflichtung auf das Maß beschränkt, das ihm infolge der drittstaatlichen Jurisdiktionsausübung über die Daten möglich ist.

In diesem Sinne hat auch der EGMR in der Entscheidung *Ilaşcu and Others v. Moldova and Russia* einen interessanten Ansatz verfolgt, der die vorliegenden Ausführungen bestätigt:

> „However, even in the absence of effective control over the Transdniestrian region, Moldova still has a positive obligation under Article 1 of the Conven-

[812] Siehe vorangegangenen Unterabschnitt B I. 2.
[813] Zur jurisdiktionsbegründenden extraterritorialen Kontrolle über Schutzobjekte siehe oben 3. Abschnitt, Unterabschnitt A. II. 4.
[814] Siehe oben 3. Abschnitt, Unterabschnitt A. II. 4. c. bb.

> tion to take the diplomatic, economic, judicial or other measures that it is in its power to take and are in accordance with international law to secure to the applicants the rights guaranteed by the Convention.“[815]

Hieraus wird deutlich, dass auch die Straßburger Richter das Bestehen von Schutzpflichten des Staates, auf dessen Gebiet infolge effektiver Kontrollausübung extraterritoriale Jurisdiktion durch einen anderen Staat begründet wird, im Grundsatz befürworten. Der Gerichtshof bringt aber eindeutig zum Ausdruck, dass der Staat nur zu den Schutzmaßnahmen verpflichtet ist, die er angesichts der Kontrollsituation auch ausführen kann.[816] Etwas genereller hat der MRA wiederum in *Concluding Observations* festgestellt, dass etwa Georgien die Umsetzung seiner Verpflichtungen aus dem IPbpR soweit wie möglich gewährleisten müsse, obwohl Russland effektive Kontrolle über georgische Gebiete ausübte.[817]

Demnach schließt die drittstaatliche Jurisdiktionsausübung über die Daten im Fall der extraterritorialen Telekommunikationsüberwachung die Schutzverpflichtung des Aufenthaltsstaates nicht von vornherein aus.

3. Schutzpflichten des Aufenthaltsstaates im Fall der extraterritorialen Telekommunikationsüberwachung

a. Schutzpflichten aus dem Recht auf Privatsphäre gemäß Art. 17 IPbpR und Art. 8 EMRK

Art. 17 Abs. 2 IPbpR enthält eine ausdrückliche Schutzpflicht, wonach Individuen einen Anspruch auf rechtlichen Schutz gegen Eingriffe in die Privatsphäre gewährt wird. Im *General Comment* 16 hat der MRA hinsichtlich der Schutzpflichten der Vertragsstaaten aus Art. 17 IPbpR folgendes ausgeführt:

> „[...] this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt

---

[815] EGMR, *Ilaşcu and Others v. Moldova and Russia* [GC], Rs. 48787/99, 8. Juli 2004, Rep. 2004-VII, Rn. 331. Auch in weiteren Fällen gegen Moldawien hat der EGMR gleichermaßen argumentiert, siehe EGMR, *Mozer v. the Republic of Moldova and Russi* [GC], Rs. 11138/10, 23. Februar 2016, Rep. 2016, Rn. 100; *Sandu and Others v. the Republic of Moldova and Russia*, Rs. 21034/05, 41569/04, 41573/04, 41574/04, 7105/06, 9713/06, 18327/06 und 38649/06, 17. Juli 2018, Rn. 34.

[816] Vgl. auch *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit, S. 1326; *Biel*, Die Europäische Menschenrechtskonvention in internationalen und nicht-internationalen bewaffneten Konflikten, S. 60 f.

[817] UN Human Rights Committee, Concluding observations: Georgia, CCPR/C/GEO/CO/3, 15. November 2007, Rn. 6. Siehe auch UN Human Rights Committee, Concluding observations: Republic of Moldova, CCPR/C/MDA/CO/2, 24. November 2009, Rn. 5.

legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[818]

Im Wortlaut von Art. 8 EMRK ist hingegen keine ausdrückliche Schutzpflicht aufzufinden. Der EGMR hat jedoch bereits 1979 in der Leitentscheidung *Marckx v. Belgium* positive Handlungspflichten erstmals aus Art. 8 EMRK ausdrücklich abgeleitet.[819] In der folgenden Spruchpraxis hat der Gerichtshof bestätigt, dass die Konventionsstaaten aus Art. 8 EMRK zu „*positive obligations*" im Einzelfall verpflichten sein können.[820] So stellte der Gerichtshof beispielsweise in der Entscheidung *X and Y v. the Netherlands* folgendes fest:

> „[...] although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life [...]. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."[821]

Als eine Ausprägung der „*positive obligations*" hat der EGMR erstmals 1981 in der Entscheidung *Young, James and Webster v. The United Kingdom*[822] Schutzpflichten aus Art. 8 EMRK abgeleitet.[823]

b. Schutzpflichtverletzung des Aufenthaltsstaates

aa. Übergriff in den Schutzbereich der Art. 17 IPbpR und Art. 8 EMRK

Wird die Telekommunikation von Individuen durch Überwachungsmaßnahmen eines Drittstaates ausgespäht, so kann die Duldung durchaus einen Übergriff im Sinne der menschenrechtlichen Schutzpflichtdogmatik darstellen. Dies setzt allerdings voraus, dass der Aufenthaltsstaat in den Überwachungsmaßnahmen des Drittstaates weder aktiv mitwirkt noch anderweitig involviert ist. Anderenfalls läge auch ein Eingriff des Aufenthaltsstaates vor, der im Rahmen der abwehrrechtlichen

---

[818] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation), 8. April 1988, Rn. 1.

[819] EGMR, *Marckx v. Belgium*, Rs. 6833/74, 13. Juni 1979, Serie A31, Rn. 31.

[820] Vgl. etwa EGMR, *Airey v. Ireland,* Rs. 6289/73, 09. Oktober 1979, Serie A 32, Rn. 31; *López Ostra v. Spain,* Rs. 16798/90, 09. Dezember 1994, Serie A 303-C, Rn. 51.

[821] EGMR, *X and Y v. the Netherlands*, Rs. 8978/80, 26. März 1985, Serie A 91, Rn. 23.

[822] EGMR, *Young, James and Webster v. The United Kingdom,* Rs. 7601/76 7806/77, 13. August 1981, Serie A 44.

[823] Vgl. auch *Grabenwarter,* European Convention on Human Rights, Art., S. 219, Rn. 72 ff.

Dimension des Schutzes der Privatsphäre zu beurteilen wäre.[824] Durch Überwachungsmaßnahmen in Form von Zugriffen auf die Telekommunikationsinfrastruktur, Beschaffungen von Telekommunikationsdaten mithilfe von *Service Providern* oder durch direkte Zugriffe auf persönliche Telekommunikationsgeräte wird die Vertraulichkeit der Korrespondenz und der persönlichen Daten empfindlich beeinträchtigt. Verletzt der Drittstaat mit diesen Maßnahmen das Recht der betroffenen Individuen auf Schutz der Privatsphäre gemäß Art. 17 IPbpR und Art. 8 EMRK, so kann aus schutzrechtlicher Perspektive kein Zweifel an dem Vorliegen eines Übergriffs vorliegen.

Übt ein Drittstaat über einen längeren Zeitraum wiederholt und dauerhaft (Massen-)Überwachungsmaßnahmen in einem Aufenthaltsstaat aus, so stellt sich die Frage, ob in solchen Fällen für das Vorliegen eines schutzrechtlichen Übergriffs in das Recht eines einzelnen Individuums die tatsächliche Korrespondenzüberwachung im Einzelfall notwendig ist oder die Gefahr der Überwachung genügt.[825] Einerseits könnte vertreten werden, dass allein die tatsächlich stattfindende konkrete Überwachung der Korrespondenz eines bestimmten Individuums und die damit verbundene Verletzung seines Rechts auf Privatsphäre durch den Drittstaat einen schutzrechtlichen Übergriff in seine Rechte darstellt. Andererseits kann aber auch auf die aus Sicht der Individuen bestehenden Dauergefahr des „Beobachtet-Werdens" abgestellt werden. Denn in solchen massiven Überwachungsszenarien kann – je nach Sachlage des konkreten Falles – wohl angenommen werden, dass über das Bestehen einer abstrakten Gefahr eines Rechtsübergriffs hinaus die Schwelle zu einer konkreten Gefahr eines Übergriffs in Form der Telekommunikationsüberwachung überschritten wird.[826] Führt ein Drittstaat dauerhaft grenzüberschreitende Massenüberwachungsprogramme in einem Aufenthaltsstaat durch, so kann letztlich kein Individuum mehr ausschließen, überwacht zu werden. Solche Überwachungspraktiken haben nicht selten eine erhebliche Selbstzensur der betroffenen Individuen und damit eine „freiwillige" Freiheitsbeschränkung zur Folge.[827] Insofern kann nach hier vertretener Auffassung die konkrete Gefahr der Überwachung in solchen weitläufigen Massenüberwachungspraktiken von Drittstaaten grundsätzlich einen Übergriff in die Rechte betroffener Individuen darstellen, ohne dass es auf die tatsächliche Durchführung von Maßnahmen im Einzelfall ankommt. Dafür spricht auch sinngemäß die Argumentation in Hinblick auf die Befürwortung des Bestehens eines Eingriffs in den Schutz der Privatsphäre aufgrund von nationalen

[824] Dabei käme auch eine Beihilfe des Aufenthaltsstaates in Betracht, siehe dazu unten Unterabschnitt B. II.

[825] Grundsätzlich kann im internationalen Menschenrechtsschutz eine *Gefährdung* für das Vorliegen einer Menschenrechtsverletzung genügen. UN Human Rights Committee, *Bordes and Temeharo* v. France, No. 645/1995, CCPR/C/57/D/645/1995, 22. Juli 1996, Rn. 5.4. Vgl. außerdem *Stahl,* Schutzpflichten im Völkerrecht, S. 155.

[826] Siehe dazu *Stahl,* Schutzpflichten im Völkerrecht, S. 159 ff.

[827] Siehe dazu bereits 2. Abschnitt, Unterabschnitt B. II. 4. d. cc.

Gesetzen zur Telekommunikationsüberwachung.[828] In extraterritorialen Kontexten kann für die Bejahung des Übergriffs nicht auf solche innerstaatlichen Rechtsnormen abgestellt werden, da diese freilich nicht außerhalb des Staates Geltung haben.[829] Die Argumentation basiert jedoch auch hier auf der bestehenden Gefahrenlage und der Unberechenbarkeit des „Beobachtet-werdens".[830] Letztlich muss auf Grundlage der konkreten Sachlage entschieden werden, ob im Einzelfall ein Übergriff aufgrund der massiven Überwachungspraxis eines Drittstaates anzunehmen ist oder nicht.

bb. Unterlassen von angemessenen Schutzmaßnahmen trotz Kenntnis des Aufenthaltsstaates über den Übergriff

Für eine Schutzpflichtverletzung käme es weiterhin darauf an, ob der Aufenthaltsstaat trotz Kenntnis über den bestehenden Übergriff keine angemessenen Schutzmaßnahmen vorgenommen hat. Hat der Aufenthaltsstaat nämlich keine Kenntnis vom Übergriff in Form der grenzüberschreitenden Überwachung, kann er auch nicht zur Vornahme von Schutzmaßnahmen verpflichtet werden.[831] Gerade im Bereich der verdeckten Überwachungsmaßnahmen der Geheimdienste kann jedoch freilich nicht ohne Weiteres davon ausgegangen werden, dass der Aufenthaltsstaat über diese Maßnahmen des Drittstaates Kenntnis hat. Die Maßnahmen werden letztlich in der Regel geheim, ohne Absprache oder Inkenntnissetzung des Aufenthaltsstaates durchgeführt. Die Kenntnis des Aufenthaltsstaates ist aber nicht per se ausgeschlossen. Solche geheimen Maßnahmen können einerseits durch die heimischen Behörden aufgedeckt werden oder aber durch involvierte Personen – wie etwa *Whistleblower* – bekannt gemacht werden. Dies kann zwar erst einige Jahre nach dem Beginn der Überwachungsmaßnahmen geschehen. Ab dem Zeitpunkt der Kenntnisgewinnung über die extraterritorialen Überwachungsmaßnahmen gegen Individuen auf seinem Hoheitsgebiet ist er jedoch grundsätzlich schutzverpflichtet. Auch in dem OHCHR-Bericht zum Schutz der Privatsphäre im digitalen Zeitalter wird die Pflicht zum Schutz der betroffenen Individuen durch den Aufenthaltsstaat anerkannt:

[828] Siehe oben 2. Abschnitt, Unterabschnitt B. I. 2.

[829] Überwachungsgesetze im Drittstaat gelten nämlich nicht im Aufenthaltsstaat.

[830] Der EGMR hat hierzu konkrete Kriterien entwickelt, die entscheiden, ob die Schwelle zum Eingriff auf Grundlage der Gesetze überschritten wird. Siehe oben 2. Abschnitt, Unterabschnitt B. I. 2. a.

[831] Hätte der Staat jedoch bei ordentlicher Sorgfaltspflichterfüllung den Übergriff kennen müssen, können indes durchaus Schutzpflichten für ihn entstehen. So im Ergebnis auch *Kälin/Künzli*, Universeller Menschenrechtsschutz, S. 125. Siehe dazu auch EGMR, *Osman v. The United Kingdom* [GC], Rs. 23452/94, 28. Oktober 1998, Rep. 1998-VIII, Rn. 116.

> „States have a duty to protect persons within their jurisdictions from extraterritorial interference with their rights to privacy, such as means of interception of communications or hacking.“[832]

cc. Umfang der Schutzpflichten des Aufenthaltsstaates

Bisher wurde aufgezeigt, dass der Aufenthaltsstaat in Fällen der extraterritorialen Telekommunikationsüberwachung gegenüber den betroffenen Individuen gemäß Art. 17 IPbpR und Art. 8 EMRK grundsätzlich schutzverpflichtet ist, sofern er von diesem Übergriff Kenntnis hat. An dieser Stelle gilt es nun den Umfang und die Grenzen der Schutzpflichten des Aufenthaltsstaates darzustellen.

(1) Weiter Ermessensspielraum des Aufenthaltsstaates

Sind die Voraussetzungen für das Bestehen menschenrechtlicher Schutzpflichten gegeben, so ist der entsprechende Staat zur Vornahme von angemessenen Maßnahmen verpflichtet. Unterlässt der Aufenthaltsstaat jegliche Maßnahmen zum Schutz der Individuen vor extraterritorialen Überwachungsprogrammen, würde er seine Schutzpflichten verletzen. Der Aufenthaltsstaat ist nämlich verpflichtet, einen Mindestschutz zu gewährleisten.[833] Hinsichtlich der Auswahl der konkreten Handlungsmaßnahmen steht dem Staat jedoch ein prinzipiell weiter Ermessensspielraum zu.[834] So ist der Aufenthaltsstaat nicht dazu verpflichtet, eine bestimmte Maßnahme durchzuführen.[835] Vielmehr kann er aufgrund seines Ermessensspielraums aus der Vielzahl möglicher Mittel eine angemessene Maßnahme wählen.[836]

Für den Schutz von Individuen vor geheimdienstlichen Überwachungsprogrammen, die von Drittstaaten innerhalb des Territoriums des Aufenthaltsstaates durchgeführt werden, sind unterschiedliche Maßnahmen denkbar, die der Aufenthaltsstaat innerhalb seiner Grenzen umsetzen könnte. Zu berücksichtigen ist hierbei, dass die Überwachungsmaßnahmen des Drittstaates auf dem Staatsgebiet des Aufenthaltsstaates zugleich einen Eingriff in dessen staatliche Souveränität

---

[832] So auch Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 25.

[833] *Stahl,* Schutzpflichten im Völkerrecht, S. 332. Die inhaltliche Dimension des konkreten Mindestmaßes hängt freilich vom in Frage stehenden Recht und den Umständen des Einzelfalles ab.

[834] EGMR, *Johnston and Others v. Ireland,* Rs. 9697/82, 18. Dezember 1986, Serie A 112, Rn. 55; *Plattform „Ärzte für das Leben“ v. Austria*, Rs. 10126/82, 21. Juni 1988, Serie A139, Rn. 34. Zur Entwicklung der Rhetorik des EGMR hinsichtlich des Beurteilungsspielraums der Konventionsstaaten siehe *Dröge,* Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 360 ff.

[835] *Stahl,* Schutzpflichten im Völkerrecht, S. 320.

[836] Die Schutzmaßnahmen müssen jedoch dem Prinzip der Verhältnismäßigkeit entsprechen. So muss der schutzverpflichtete Staat in der Auswahl und der konkreten Durchführung der Maßnahme darauf Acht geben, dass die menschenrechtlichen Grundsätze der Verhältnismäßigkeit beachtet werden.

bedeuten könnten.[837] In völkerrechtlicher Hinsicht wäre der Aufenthaltsstaat dann zu ausnahmsweise gerechtfertigten Gegenmaßnahmen befugt. In Betracht kämen dann beispielsweise diplomatische Maßnahmen, Strafverfolgungsmaßnahmen oder die Aberkennung des diplomatischen Status von drittstattlichen Diplomaten im Aufenthaltsstaat.

In Fällen des drittstaatlichen Zugriffs auf die Telekommunikationsinfrastruktur, die sich innerhalb des Territoriums des Aufenthaltsstaates befindet,[838] kämen konkret etwa präventive Maßnahmen in Betracht. So könnte möglicherweise mithilfe technischer oder mechanischer Hilfsmittel der Übergriff auf die Infrastruktur zumindest erschwert werden. Des Weiteren könnten Aufsichtsmechanismen eingeführt werden, die etwa den ungestörten Datenfluss durch die Telekommunikationsinfrastruktur zumindest innerhalb des eigenen Staatsgebiets kontrollieren.[839] Auch für den Fall der geheimdienstlichen Informationsbeschaffung durch Zugriffe auf Server von *Service Providern*, die innerhalb des Staatsgebiets des Aufenthaltsstaates ansässig sind, kommen unterschiedliche Maßnahmen in Betracht. So könnten durch den Gesetzgeber beispielsweise Strafvorschriften erlassen werden, die die Kooperation von Internetdienstleistern mit ausländischen Geheimdiensten unter Strafe stellt. Damit könnten zumindest die Überwachungsprogramme eingedämmt werden, die von der freiwilligen Kooperation der Internetdienstleister abhängen.[840] Hinsichtlich des geheimdienstlichen Direktzugriffs auf privatgenutzte Telekommunikationsgeräte könnte der Aufenthaltsstaat zum Beispiel durch öffentliche Warnungen die Nutzer auf geheimdienstliche Hackerangriffe durch Drittstaaten – etwa in Form versteckter Viren in Emailanhängen – aufmerksam machen.

Sicherlich kann hinsichtlich all der aufgeführten Beispiele zurecht hinterfragt werden, ob und inwieweit diese praktisch einen effektiven Schutz vor grenzüberschreitenden Überwachungsmaßnahmen gewähren können.[841] Der Aufenthaltsstaat ist jedoch im Rahmen der ihm obliegenden Schutzpflichten nicht dazu verpflichtet, jegliche Übergriffe in Form von ausländischen Überwachungsmaß-

---

[837] Vgl. zur Frage der Verletzung der Staatssouveränität durch Spionagemaßnahmen *Kittichaisaree*, Public International Law of Cyberspace, S. 241 ff. Zu der im Völkerrecht gewohnheitsrechtlich anerkannten Staatssouveränität siehe Von *Arnauld*, Souveränität als fundamentales Konzept des Völkerrechts, S. 51 ff.

[838] Hierunter fallen etwa Fälle, in denen der Drittstaat Daten aus Glasfaserkabeln abfängt, die sich innerhalb des Territoriums des Aufenthaltsstaates befinden.

[839] So könnten beispielsweise Behörden eingerichtet werden, die speziell zur gezielten Kontrolle der empfindlichen Internetdatentransferkabel beauftragt werden. Sind etwa Unterseekabel, die sich nicht auf hoher See befinden, sondern noch im Küstengebiet des Staates liegen, von ausländischen Hackerangriffen betroffen, wären regelmäßige Kontrollen durch U-Boote möglich.

[840] Verdeckte Hackerangriffe auf die Server von *Service Provider* würden durch solche Gesetze freilich nicht eingedämmt werden.

[841] Gerade im Bereich der Anwendung von technischen Vorrichtungen zur Erschwerung von Überwachungsakten ausländischer Geheimdienste können die Aufenthaltsstaaten mit der technischen Überlegenheit der Drittstaaten konfrontiert sein. In solchen Fällen kann der Aufenthaltsstaat solche Übergriffe kaum wirksam verhindern.

nahmen absolut zu verhindern.[842] Vielmehr ist er nur zur Vornahme angemessener Maßnahmen verpflichtet. Sofern also trotz der Vornahme angemessener Schutzmaßnahmen Menschenrechtsbeeinträchtigungen aufgrund des Übergriffs eintreten, so liegt keine Schutzpflichtverletzung des Staates vor.[843] Das Schutzpflichtmaß des Aufenthaltsstaates kann zudem aufgrund einer tatsächlichen Unmöglichkeit begrenzt sein.[844] Gerade im vorliegenden Fall des Schutzes vor geheimdienstlicher Überwachung durch Drittstaaten können technische Maßnahmen – etwa zur Kontrolle der störungsfreien Abwicklung des Datenverkehrs im Telekommunikationsnetz – mit erheblich hohen Kosten verbunden sein. Der Aufenthaltsstaat kann nur zur Durchführung von Maßnahmen verpflichtet sein, die ihm auch finanziell möglich sind.[845] Tatsächlich möglich und wohl insgesamt eher realitätsnah sind hingegen diplomatische Schutzmaßnahmen.[846]

(2) Verhältnismäßigkeit der konkreten Maßnahme

Das Prinzip der Verhältnismäßigkeit[847] gilt in modifizierter Form auch für Schutzrechte.[848] Denn auch im Rahmen von staatlichen Schutzpflichten muss ein gerechter Interessenausgleich zwischen den Interessen des Staates und dem Schutzinteresse des Individuums bestehen.[849] Die in Schutzpflicht-Konstellationen vom Staat ergriffenen Maßnahmen müssen demnach ein legitimes Ziel verfolgen und den Grundsätzen der Geeignetheit, Erforderlichkeit und Angemessenheit entsprechen. Die Schutzmaßnahmen sind in diesem Sinne geeignet, wenn der wirksame Schutz des infrage stehenden Menschenrechts des betroffenen Individuums zumindest

---

[842] EGMR, *Plattform „Ärzte für das Leben" v. Austria,* Rs. 10126/82, 21. Juni 1988, Serie A139, Rn. 34. Siehe außerdem *Stahl,* Schutzpflichten im Völkerrecht, S. 317 m.w.N.

[843] Ebd., S. 318.

[844] Ebd., S. 321 ff.

[845] Dazu Ebd., S. 321 f.

[846] Dazu sogleich im Unterabschnitt B. I. 3. b. cc. (3). Siehe außerdem *Stahl,* Schutzpflichten im Völkerrecht, S. 330.

[847] Im deutschen Rechtsraum wird für den Grundsatz der Verhältnismäßigkeit im Rahmen von Schutzpflichten der Begriff „Untermaßverbot" als Äquivalent zum abwehrrechtlichen „Übermaßverbot" verwendet. *Störring,* Das Untermaßverbot in der Diskussion, S. 21 ff.

[848] *Stahl,* Schutzpflichten im Völkerrecht, S. 330.

[849] Der EGMR prüft auch im Rahmen von Schutzpflichten die Verhältnismäßigkeit unter der Bezeichnung *„fair-balance-test"*. Dabei stellt er zuvor nicht fest, ob es sich um eine abwehrrechtliche oder schutzrechtliche Konstellation handelt. Vielmehr prüft er die Verhältnismäßigkeit mit der Begründung vorab, dass in beiden Fällen für die Verhältnismäßigkeit gleiche Prinzipien gelten und letztlich eine Abwägung der Interessen des betroffenen Individuums und der entgegenstehenden (Staats-)Interessen vorgenommen werden müsse. So etwa in EGMR, *Keegan v. Ireland,* Rs. 16969/90, 26. Mai 1994, Serie A 290, Rn. 49: „The applicable principles are, none the less, similar. In both cases regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole; and in both contexts the State enjoys a certain margin of appreciation (…)."

gefördert wird.[850] Erforderlich ist eine Schutzmaßnahme zudem, wenn kein anderes Mittel das Schutzziel besser verwirklichen würde, ohne dabei stärker die entgegenstehenden Interessen zu beschränken.[851] Im Rahmen der Angemessenheit ist das geförderte Schutzinteresse mit den Beeinträchtigungen der entgegenstehenden Interessen abzuwägen.[852] So gilt es an dieser Stelle letztlich einen angemessenen Ausgleich zwischen dem Schutzinteresse des betroffenen Individuums und den entgegenstehenden Interessen der Allgemeinheit oder Dritter zu finden:

> „In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which balance is inherent in the whole of the Convention“.[853]

In extraterritorialen Überwachungsfällen gelten die Maßstäbe dieses (modifizierten) Verhältnismäßigkeitsgrundsatzes freilich auch für das Pflichtprogramm des Aufenthaltsstaates. Dieser muss demnach hinsichtlich der Auswahl und Durchführung von Maßnahmen zum Schutze der Individuen vor den drittstaatlichen Spionagemaßnahmen diese Grundsätze beachten. Dabei steht in der zentralen Angemessenheitsabwägung einerseits das Schutzinteresse der betroffenen Individuen hinsichtlich der Vertraulichkeit ihrer Korrespondenz und der personenbezogenen Daten gemäß Art. 17 IPbpR und Art. 8 Abs. 1 EMRK. Auf der anderen Seite stehen die der Allgemeinheit und dem Staatswohl dienenden Interessen des Aufenthaltsstaates selbst. Dabei sind hier bestimmte Interessen des Aufenthaltsstaates relevant, die – aus Sicht des Aufenthaltsstaates – gegen sehr umfangreiche Schutzmaßnahmen sprechen, obwohl diese einen weitreichenderen Schutz der Individualinteressen bewirken würden. Beispielsweise kann der Aufenthaltsstaat aufgrund finanzieller Erwägungen und angesichts der wirtschaftlichen Lage des Staates die Schutzmaßnahmen auf ein begrenztes und finanziell tragbares Maß reduzieren.[854] Außerdem könnten etwa Erwägungen hinsichtlich des zwischenstaatlichen Verhältnisses mit dem Drittstaat gegen bestimmte Schutzmaßnahmen sprechen. Dabei sei an dieser Stelle darauf hingewiesen, dass gerade im Bereich diplomatischer Fragen den Staaten zweifellos ein äußerst weiter Ermessensspielraum zukommt.[855] In diesen Beispielsfällen stünden dem Schutzinteresse der Individuen wirtschaftliche oder außen-

---

[850] *Dröge,* Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 311.
[851] Ebd.
[852] *Stahl,* Schutzpflichten im Völkerrecht, S. 312.
[853] EGMR, *Rees v. The United Kingdom*, Rs. 9532/81, 17. Oktober 1986, Serie A 106, Rn. 37.
[854] Ohne dass bereits die Grenze der finanziellen Unmöglichkeit erreicht wird, kann der Staat auch innerhalb des tatsächlich Möglichen die Mittel wählen, die in finanzieller Hinsicht weniger belastend sind. Siehe auch *Dröge,* Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, S. 312.
[855] Siehe auch *Stahl,* Schutzpflichten im Völkerrecht, S. 304.

politische Interessen des Aufenthaltsstaates entgegen, die letztlich zum Wohle der Allgemeinheit in Bezug auf die Auswahl der konkreten Schutzmaßnahmen vom Aufenthaltsstaat berechtigterweise in Erwägung gezogen werden.

Somit darf die angewendete Schutzmaßnahme aufgrund des Grundsatzes der Verhältnismäßigkeit einerseits nicht zu schwach und geringfügig sein. Die Maßnahme muss vielmehr einen *verhältnismäßig* wirksamen Schutz der menschenrechtlichen Individualinteressen gewähren. Auf der anderen Seite setzt der Verhältnismäßigkeitsgrundsatz im komplexen Fall der extraterritorialen Telekommunikationsüberwachung auch eine Obergrenze für das Pflichtmaß des Aufenthaltsstaates. Denn die Interessen des Aufenthaltsstaates werden im Rahmen der Angemessenheit gebührend gewichtet und zur Erreichung eines *angemessenen* Ausgleiches mit dem Schutzinteresse der Individuen aufgewogen.

(3) Diplomatische Maßnahmen

Im Rahmen drittstaatlicher Übergriffe – wie etwa der extraterritorialen Telekommunikationsüberwachung – stehen diplomatische Schutzmaßnahmen als Mittel erster Wahl im Vordergrund. In der oben bereits zitierten Begründung der Entscheidung *Ilaşcu and Others v. Moldova and Russia* hat auch der EGMR in seiner Auflistung möglicher Maßnahmen, die Moldawien trotz fehlender Jurisdiktionsausübung auf seinem Staatsgebiet gegen Russland durchführen kann, „*diplomatic [...] measures*" an erster Stelle genannt.[856]

Dabei kommt zunächst die Ausübung diplomatischen Schutzes i.e.S. in Betracht. Die ILC definiert in Art. 1 der 2006 angenommenen *draft articles on diplomatic protection* den diplomatischen Schutz i.e.S. folgendermaßen:

> „diplomatic protection consists of the invocation by a State, through diplomatic action or other means of peaceful settlement, of the responsibility of another State for an injury caused by an internationally wrongful act of that State to a natural or legal person that is a national of the former State with a view to the implementation of such responsibility." [857]

Ein Staat kann nach Völkergewohnheitsrecht diplomatischen Schutz zugunsten eigener Staatsangehöriger ausüben, die aufgrund eines völkerrechtlichen Delikts des anderen Staates in ihren Rechten verletzt werden.[858] Der Staat, dessen Staatsangehörigkeit das verletzte Individuum besitzt, kann die völkerrechtliche Verantwortlichkeit des anderen Staates geltend machen, etwa indem er die Durchführung von

---

[856] EGMR, *Ilaşcu and Others v. Moldova and Russia* [GC], Rs. 48787/99, 8. Juli 2004, Rep. 2004-VII, Rn. 331.

[857] Report of the International Law Commission, Fifty-eighth session (2006), General Assembly Official Records A/61/10, S. 16.

[858] Siehe dazu Art. 1 der *draft articles on diplomatic protection* der ILC, Report of the International Law Commission, Fifty-eighth session (2006), General Assembly Official Records A/61/10, S. 16; *Amerasinghe,* Diplomatic Protection, S. 25 ff.

Verfahren oder Verhandlungen zur Untersuchung und Wiedergutmachung verlangt.[859]

In Fällen der extraterritorialen Telekommunikationsüberwachung können die Rechte der überwachten Individuen aus Art. 17 IPbpR und Art. 8 EMRK durch die Überwachungsmaßnahmen des Drittstaates verletzt sein. In diesem Fall stellt die Verletzung von Menschenrechten aus der EMRK und dem IPbpR einen völkerrechtswidrigen Akt des überwachenden Drittstaates dar. Weitere Voraussetzung für den diplomatischen Schutz ist, dass das betroffene Individuum Staatsangehöriger des Heimatstaates ist.[860] Das bedeutet für den Fall der Telekommunikationsüberwachung, dass der Aufenthaltsstaat diplomatischen Schutz nur für die Individuen, die seine Staatsangehörige sind, ausüben kann.[861] Dies schränkt die Reichweite der Schutzwirkung für diesen Fall ein. Denn Extraterritoriale (Massen-) Überwachungsmaßnahmen zielen nicht darauf ab, nur Staatsangehörige des Aufenthaltsstaates zu beobachten. Vielmehr werden grundsätzlich jegliche Korrespondenzen und Daten erfasst, ohne dass dabei vorab eine Beschränkung auf Personen mit einer bestimmten Staatsangehörigkeit vorgenommen wird. Denn im Aufenthaltsstaat werden zwar überwiegend die Staatsangehörigen desselben leben, darüber hinaus aber auch andere Staatsangehörige.

Neben dem diplomatischen Schutz kommen eine Reihe anderer diplomatischer Maßnahmen in Betracht, die der Aufenthaltsstaat in Erfüllung seiner menschenrechtlichen Schutzpflichten ausführen könnte. Der Aufenthaltsstaat könnte den Drittstaat etwa auf die Menschenrechtsverletzung infolge der Überwachung aufmerksam machen und ein ausdrückliches Abhilfeverlangen formulieren. Damit verbunden könnte der Aufenthaltsstaat zur Beendigung solcher Maßnahmen gegen

---

[859] Vgl. dazu *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit, S. 1281.

[860] In klassischen Fällen diplomatischen Schutzes befindet sich das Individuum auf dem Staatsgebiet des Staates, das den völkerrechtwidrigen Akt vorgenommen hat. Dies ist bei grenzüberschreitenden Überwachungen nicht der Fall, befinden sich doch die überwachten Individuen im Aufenthaltsstaat. Dies schließt jedoch die Ausübung diplomatischen Schutzes für die eigenen Staatsangehörigen nicht aus. Denn vorausgesetzt ist nur die Staatsangehörigkeit, nicht jedoch der Aufenthalt des Individuums außerhalb des eigenen Staates. Dies geht sinngemäß auch aus dem *Diallo*-Urteil des IGH hervor, International Court of Justice, Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo), Merits, Judgment, I.C.J. Reports 2010, S. 639.

[861] Vom Grundsatz der Staatsangehörigkeit im Rahmen des diplomatischen Schutzes gibt es zwar anerkannte Ausnahmen. Diese greifen aber nicht im Fall der Telekommunikationsüberwachung. Vgl. dazu *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit, S. 1285 ff. Im Gegensatz zum diplomatischen Schutz erstrecken sich die menschenrechtlichen Schutzpflichten des Aufenthaltsstaates auf alle betroffenen Individuen auf dem eigenen Staatsgebiet, ohne dass es auf die Staatsangehörigkeit ankommt. So auch *Stahl*, Schutzpflichten im Völkerrecht, S. 132. Denn die Verpflichtung der Staaten im internationalen Menschenrechtsschutz knüpft nicht an die Staatsangehörigkeit an, sondern richtet sich nach der Jurisdiktionsausübung der Staaten. Dies geht aus den Art. 2 Abs. 1 IPbpR und Art. 1 EMRK hervor. Das Konzept des diplomatischen Schutzes, das grundsätzlich die Staatsangehörigkeit als Kriterium voraussetzt und den Schutz von Staatsangehörigen im Ausland betrifft, beruht auf anderen völkerrechtlichen Grundsätzen. Siehe hierzu *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit, S. 1283.

Individuen in seinem Territorium auffordern. Des Weiteren käme als striktere Maßnahme auch die konsequente Ausübung politischen Drucks in Betracht.[862] Neben diesen einseitigen, vom Aufenthaltsstaat ausgehenden Maßnahmen könnte dieser auch auf den Abschluss eines völkerrechtlichen Vertrages hinwirken. Hierin könnten sich beide Parteien dazu verpflichten, Überwachungsmaßnahmen auf den gegenseitigen Staatsgebieten zu unterlassen.

Der Aufenthaltsstaat verfügt freilich hinsichtlich der Auswahl aus solchen diplomatischen Mitteln einen weiten Ermessensspielraum.[863] Betroffene Individuen können vom Aufenthaltsstaat nicht verlangen, konkrete diplomatische Vorgehensweisen durchzuführen.[864] Der Aufenthaltsstaat ist indes dazu verpflichtet ermessensfehlerfrei über die Auswahl seiner diplomatischen oder sonstigen Schutzmaßnahmen zu entscheiden. Jedenfalls ist der Aufenthaltsstaat aber im Rahmen seiner Schutzverpflichtung dazu verpflichtet, den menschenrechtlich vorgeschriebene Mindestschutz zu gewährleisten. In Erfüllung dieser Pflicht sind solche diplomatischen Maßnahmen jedenfalls naheliegend. Sicherlich drängt sich hier trotz allem die Frage auf, ob und inwieweit solche Maßnahmen letztlich wirksam sind. So kann der Drittstaat ungeachtet solcher diplomatischen Aufforderungen an der Fortführung seiner Überwachungsprogramme festhalten. Ob der Aufenthaltsstaat in der Konsequenz wiederum schärfere Mittel wählt, um dem Schutzinteresse betroffener Individuen abzuhelfen, unterliegt gleichsam seinem Ermessen.

4. Ergebnis

Nicht nur der Drittstaat kann aufgrund seiner extraterritorial durchgeführten Telekommunikationsüberwachung die Rechte aus Art. 17 IPbpR und Art. 8 EMRK verletzen, sondern auch der unbeteiligte Aufenthaltsstaat. Denn bei Vorliegen aller Voraussetzungen ist dieser zum Schutz der betroffenen Individuen verpflichtet. Die extraterritoriale Jurisdiktionsausübung des Drittstaates über die Telekommunikationsdaten schließt diese menschenrechtliche Schutzverpflichtung indes nicht aus. Im Rahmen seines weiten Ermessenspielraums muss der Aufenthaltsstaat einen angemessenen (Mindest-)Schutz gewähren. Die Tatsache, dass der Übergriff durch einen Drittstaat hervorgeht, erschwert freilich eine effektive Schutzgewährung. In der Praxis werden wohl in erster Linie diplomatische Maßnahmen in Betracht kommen. Die Umsetzung diplomatischer Mittel könnten aber genügen, um die Schutzpflichten aus Art. 17 IPbpR und Art. 8 EMRK zu erfüllen. Ob diese diplomatischen Mittel allerdings eine Beendigung der Überwachungsmaßnahmen seitens des Drittstaates zur Folge hätten, ist unbestritten zu bezweifeln.

---

[862] *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit, S. 1280.

[863] Zum weiten Ermessenspielraum siehe bereits oben Unterabschnitt B. I. 3. b. cc. (1).

[864] So hat auch die EKMR bereits im Fall *Dobberstein v. Germany,* Rs. 25045/94, 12. April 1994 entschieden; ebenso in den Fällen *Luck v. Germany*, Rs. 24928/94, 30. November 1994; *Jüngling and Others v. Germany,* Rs. 22353/93, 18. Oktober 1995; *Nadler and Reckziegel v. Germany,* Rs. 27718/95, 12. April 1996. Vgl. zu diesem Thema außerdem *Stahl,* Schutzpflichten im Völkerrecht, S. 1344.

II. Verantwortlichkeit des Aufenthaltsstaates durch Beihilfe

Der Aufenthaltsstaat kann weiterhin aufgrund von Beihilfehandlungen zugunsten der Überwachungsmaßnahmen eines Drittstaates verantwortlich sein.[865] Dabei handelt es sich um Fallkonstellationen, in denen der Aufenthaltsstaat durch bewusste Hilfshandlungen die drittstaatliche Überwachung der Individuen auf seinem Staatsgebiet unterstützt und damit als fördernder Faktor in dieser menschenrechtlichen Eingriffshandlung involviert ist. Dabei kommen vielfältige Hilfeleistungen des Aufenthaltsstaates, die letztlich den Weg für eine ungestörte Überwachung von Individuen im Aufenthaltsstaat durch den Drittstaat freimachen, in Betracht. So kann der Aufenthaltsstaat beispielsweise bewusst mechanische oder technische Barrieren, die die innerstaatliche Telekommunikationsinfrastruktur vor Übergriffen schützen sollen, aufheben. Damit würde er die Ausspähung des durchfließenden Datenverkehres für den Drittstaat erheblich erleichtern. Auch die Weitergabe von Korrespondenzdaten oder strategischen Informationen – etwa über den Standort von innerstaatlichen Datenkabeln und -knotenpunkten – können für ausländische Geheimdienste durchaus wertvoll sein. Der Aufenthaltsstaat unterstützt und erleichtert durch diese Handlungen die menschenrechtliche Eingriffshandlungen des Drittstaates. Fraglich ist allerdings, inwieweit diese Hilfsleistungen die völkerrechtliche Staatenverantwortlichkeit des Aufenthaltsstaates auslösen. Die völkerrechtlich unverbindlichen ILC-Artikelentwürfe zur Staatenverantwortlichkeit[866] enthalten in Art. 16 einen Tatbestand zur völkerrechtlichen Beihilfe, der solche und ähnliche Hilfshandlungen des Aufenthaltsstaates erfassen könnte:

> „Article 16. Aid or assistance in the commission of an internationally wrongful act
>
> A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:
>
> (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and
>
> (b) the act would be internationally wrongful if committed by that State."

Der IGH hat 2007 in dem Urteil zum Völkermord in Srebrenica Art. 16 des ILC-Entwurfs als geltendes Völkergewohnheitsrecht angesehen.[867]

---

[865] Siehe dazu auch EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 495.

[866] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, A/56/10 (2001), S. 26.

[867] International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment (2007) I.C.J Reports 2007, S. 150, Rn. 417 ff.

Aus dem Wortlaut des zitierten Artikelentwurfs gehen die Voraussetzungen für eine Begründung der Staatenverantwortlichkeit aufgrund von Beihilfe hervor. So setzt Art. 16 einerseits voraus, dass eine völkerrechtswidrige Tat durch den unterstützten Staat vorliegen muss. Der helfende Staat muss durch Unterstützungshandlungen die Tat des anderen Staates fördern. Dabei muss er in Kenntnis über die rechtswidrige Tat des unterstützten Staates handeln. Des Weiteren setzt Art. 16 voraus, dass die Tat auch dann rechtwidrig wäre, wenn sie vom unterstützenden Staat selbst ausgeführt werden würde. Letztlich bedeutet dies, dass der beihilfeleistende Staat an die Völkerrechtsnorm, gegen die der andere Staat durch seine Handlung verstoßen hat, ebenfalls gebunden ist.

Die grenzüberschreitende Telekommunikationsüberwachung durch den Drittstaat kann seine extraterritoriale Jurisdiktion über die Telekommunikationsdaten als menschenrechtlich geschützte Schutzobjekte begründen.[868] In der Folge ist der Drittstaat – wie im vorangegangenen Unterabschnitt ausführlich dargelegt[869] – an seine Menschenrechtsverpflichtungen aus den Art. 17 IPbpR und Art. 8 EMRK gegenüber den Individuen im Aufenthaltsstaat gebunden. Sind die Überwachungsmaßnahmen indes nicht in dem von Art. 17 IPbpR und Art. 8 EMRK niedergelegten Rahmen gerechtfertigt, so würde der Drittstaat mithin diese Menschenrechte der betroffenen Individuen verletzen. Diese Menschenrechtsverletzung stellt zudem eine Verletzung der völkerrechtlichen Verpflichtung des Drittstaates, der die jeweiligen Menschenrechtspakte unterzeichnet und ratifiziert hat, dar. Somit würde in diesem Fall eine völkerrechtswidrige Handlung des Drittstaates – wie von Art. 16 des ILC-Entwurfs vorausgesetzt – vorliegen. Weiterhin wurde bereits eingangs aufgezeigt, dass bestimmte Handlungen des Aufenthaltsstaates die Durchführung der drittstaatlichen Überwachung fördern würden. So wurde beispielsweise auf die Weitergabe von strategischen Informationen über die inländische Telekommunikationsinfrastruktur verwiesen. Jegliche Handlungen des Aufenthaltsstaates, die Überwachungsmaßnahmen durch den Drittstaat erleichtern, können als fördernde Beihilfeleistungen in Betracht kommen.

Der Aufenthaltsstaat müsste jedoch in Kenntnis der völkerrechtswidrigen Tat handeln. Der ILC hat in seinem Kommentar zu den entworfenen Artikeln festgestellt, dass „A State is not responsible for aid or assistance under article 16 unless the relevant State organ intended [...] to facilitate the occurrence of the wrongful conduct".[870]

Daraus geht hervor, dass neben dem reinen Wissen über den völkerrechtswidrigen Akt auch eine subjektive Intention – ein „Wollen" – zur Unterstützung des

[868] Zur Jurisdiktionsausübung aufgrund extraterritorialer Kontrolle über Schutzobjekte siehe oben 3. Abschnitt, Unterabschnitt A. II. 4.

[869] Siehe Unterabschnitt A. II. 4. c. cc.

[870] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, A/56/10 (2001), S. 66, ILC Commentary to Article 16 of the Articles on State Responsibility, Rn. 5.

Aktes auf Seiten des helfenden Staates gegeben sein muss.[871] Die hier untersuchten Unterstützungshandlungen des Aufenthaltsstaates für den überwachenden Drittstsaat erfolgen bewusst, sodass auch das subjektive Element erfüllt wäre.

Um eine Verantwortlichkeit des Aufenthaltsstaates aufgrund von Beihilfe gem. Art. 16 des ILC-Entwurfs zu begründen, müsste dieser zudem unter demselben Menschenrechtsvertrag, an den der Drittstaat gebunden ist, verpflichtet sein. Verletzt der Drittstaat beispielsweise den Art. 17 IPbpR durch seine Überwachungsmaßnahmen, so wäre eine Verantwortlichkeit des Aufenthaltsstaates im Sinne des Art. 16 nur möglich, wenn auch der Aufenthaltsstaat an den IPbpR gebunden ist.

C. Menschenrechtsverletzung durch *Intelligence Sharing*

Zum Thema der grenzüberschreitenden Telekommunikations-überwachung gehören auch zwischenstaatliche Vereinbarungen zum Austausch von geheimdienstlichen Informationen. Diese gemeinhin unter der Bezeichnung „*Intelligence Sharing*“ bekannte Praxis ist heute keineswegs unüblich.[872] Dabei vereinbaren zwei oder mehrere Staaten, dass sie Telekommunikationsdaten, die ihre Geheimdienste durch innerstaatliche oder grenzüberschreitende Überwachungsmaßnahmen gewonnenen haben, anderen Staaten zur weiteren Analyse und Auswertung zur Verfügung stellen. Es gibt zahlreiche Abkommen dieser Art, wobei einige mehr und andere weniger bekannt sind.[873] Der zwischenstaatliche Informationsaustausch erfolgt nicht immer auf Grundlage umfassender und formaler Verträge, sondern wird häufig auch auf informeller Basis zwischen zwei Staaten abgewickelt, ohne dass es einen beständigen Vertrag hierfür gäbe.[874] Grundsätzlich sind die Details und konkreten Strukturen solcher Verträge und Abreden geheim.[875] Das wohl bekannteste Abkommen

[871] Diese Ansicht wird auch in der Literatur überwiegend vertreten: Siehe etwa *Aust,* The UN Human Rights Due Diligence Policy, S. 237 ff.; *Dominicé,* Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State, in Crawford/Pellet/Olleson (Hrsg.), The Law of International Responsibility, S. 286. Auch der ehemalige Berichterstatter der ILC hat sich dafür ausgesprochen, dass der helfende Staat durch seine Hilfshandlung die Durchführung der völkerrechtswidrigen Tat auch unterstützen wolle, siehe *Crawford,* The International Law Commission’s Articles on State Responsibility, S. 408. Die Gegenmeinung in der Literatur sagt jedoch, dass eine subjektive Komponente die Anwendung des Art. 16 sehr beschränken würde. Denn der Nachweis, dass ein Staat vorsätzlich die völkerrechtswidrige Tat eines anderen Staates unterstützen wollte, wäre in der Praxis kaum erbringbar: *Niebank,* Menschenrechtliche Grenzen der zwischenstaatlichen Kooperation, S. 14. *Moynihan* vertritt eine vermittelnde Ansicht, wonach für das voluntative Element des Art. 16 eine „willentliche Blindheit“ seitens des helfenden Staates genüge, *Moynihan*, Aiding and Assisting, S. 471.

[872] Vgl. dazu aus deutscher Rechtsperspektive *Schaller*, Strategic Surveillance and Extraterritorial Basic Rights Protection, S. 959 f.

[873] Für eine Übersicht über einige *Intelligence-Sharing*-Abkommen siehe etwa *Lefebvre*, The Difficulties and Dilemmas of International Intelligence Cooperation, S. 529 ff.

[874] Vgl. dazu *Sepper,* Democracy, Human Rights, and Intelligence Sharing, S. 156 ff.

[875] Ebd., S. 156.

zum zwischenstaatlichen Austausch von geheimdienstlichen Informationen ist das *UKUSA Agreement* von 1947, das auch „*five eyes*" genannt wird. In diesem Vertrag haben sich die USA, das Vereinigte Königreich, Australien, Kanada und Neuseeland zur Zusammenarbeit ihrer Geheimdienste verpflichtet.[876]

Der Informationsaustausch auf Grundlage solcher Vereinbarungen kann im Einzelfall menschenrechtswidrig sein. Denn unabhängig von dem vorausgegangenen Akt der Datenausspähung können auch die Weitergabe und der Erhalt der ausgespähten Daten eigenständige Eingriffe in die Rechte aus Art. 17 IPbpR und Art. 8 EMRK darstellen. Der MRA und der EGMR sind erst in jüngster Zeit mit der Frage nach der Menschenrechtskonformität des *Intelligence Sharings* konfrontiert. In den bisherigen Stellungnahmen zu dieser Problematik haben sie durchaus zu erkennen gegeben, dass der Datentransfer – unabhängig von der vorangegangenen Ausspähung – eine eigenständige Eingriffshandlung in die Rechte aus Art. 17 IPbpR und Art. 8 EMRK darstellt.

Im Fall *Big Brother Watch and Others v. The United Kingdom* befasst sich der EGMR erstmals mit dem Thema *Intelligence Sharing*. Die Große Kammer hat in diesem Fall den Erhalt sowie die nachfolgende Speicherung und Verarbeitung der Daten als Eingriffshandlung qualifiziert.[877]

Für die Rechtfertigung dieser Akte gelten im Grundsatz die gleichen Anforderungen. Das Recht auf Vertraulichkeit der Korrespondenz und der Daten besteht fort, auch wenn bereits zuvor Kenntnis durch einen Staat erlangt wurde. Aus menschenrechtlicher Sicht darf es nämlich keine Rolle spielen, dass ein Staat die Daten nicht selbst durch eigene Überwachungsmaßnahmen erlangt, sondern diese vielmehr aufgrund von zwischenstaatlichen Vereinbarungen erhält. So muss auch in Fällen von *Intelligence Sharing* der von Art. 17 IPbpR und Art. 8 EMRK vorgegebene und in der Spruchpraxis des MRA und des EGMR weiterentwickelte rechtliche Rahmen für den Staat, der die Daten empfängt und weiterverarbeitet, gleichermaßen gelten. Die strengen Überwachungsregulierungen in einem Staat könnten anderenfalls umgangen werden, indem Informationen von anderen Staat eingeholt werden, in denen die Telekommunikationsdaten mit menschenrechtswidrigen Mitteln ausgespäht wurden.[878] So hat in diesem Sinne auch die *Venice Commission* zu

---

[876] Ebd., S. 157; *Lefebvre*, The Difficulties and Dilemmas of International Intelligence Cooperation, S. 530. Auf EU-Ebene wurde mit Europol eine Plattform zum Austausch von Informationen zwischen den Mitgliedstaaten geschaffen, siehe dazu *Ballaschk,* In the Unseen Realm. Transnational Intelligence Sharing in the European Union, S. 37 ff.

[877] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 496.

[878] Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 21; EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 497. Außerdem *Sepper,* Democracy, Human Rights, and Intelligence Sharing, S. 180 f.

dieser Problematik in einem einschlägigen Bericht Stellung bezogen.[879] Demnach dürften die von einem anderen Staat ausgespähten Daten nur dann analysiert und verwendet werden, wenn die ursprüngliche Ausspähung und Datengewinnung alle im eigenen Staat geltenden rechtlichen Anforderungen der Telekommunikationsausspähung erfüllen. Menschenrechtswidrig erlangte Daten dürften demzufolge auch von einem Staat, der diese nicht selbst ausgespäht hat, nicht verarbeitet werden.[880]

Dieser Argumentation scheint auch der EGMR in seinem Urteil durch die im Fall *Big Brother Watch and Others v. The United Kingdom* zu folgen.[881] Auch der MRA setzt für die Bewertung von transnationalen Praktiken des Transfers von ausgespähten Telekommunikationsdaten bisher das übliche Maß an, das auch für die Ausspähung gilt.[882]

Der zwischenstaatliche Informationsaustausch muss außerdem in den involvierten Staaten gesetzlich normiert sein. Auch hier dient das Erfordernis der gesetzlichen Grundlage dem Schutz vor Machtmissbrauch.[883] So müssen die Gesetze in den involvierten Staaten den Grundsätzen der „*Accessibility*“ und „*Foreseeability*“, d.h. der Zugänglichkeit und Bestimmtheit, genügen. Im speziellen Fall des *Intelligence Sharing* bedeutet das konkret, dass das zugrundeliegende Gesetz in dem jeweiligen Staat die Umstände, unter denen die Herausgabe, der Empfang oder der Austausch von Telekommunikationsdaten durchgeführt werden kann, ausführlich niedergelegt sein müssen. Außerdem müssen auch hier konkrete Regelungen über die Speicherung, Verarbeitung sowie Löschung der Daten vorhanden sein. Außerdem sind auch im Fall des zwischenstaatlichen Informationsaustausches Regelungen über den weiteren Datentransfer erforderlich.[884]

Weiterhin müssen die Anforderungen an die Verhältnismäßigkeit, wie sie vom MRA und dem EGMR in ihrer Spruchpraxis zur Menschenrechtskonformität von geheimdienstlichen Maßnahmen zur Telekommunikationsüberwachung entwickelt wurden, auch im Bereich des geheimdienstlichen Informationsaustausches erfüllt sein. Die Verhältnismäßigkeit des *Intelligence Sharings* hängt insofern im Einzelfall

---

[879] European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democracy Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies (CDL-AD(2015)006), Venice, March 2015.
[880] Ebd., Rn. 73.
[881] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 497.
[882] UN Human Rights Committee, Concluding observations: Sweden, CCPR/C/SWE/CO/7, 28. April 2016, Rn. 37; Concluding observations: United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17. August 2015, Rn. 24; Concluding observations: Canada, CCPR/C/CAN/CO/6, 13. August 2015, Rn. 10; Concluding observations: Pakistan, CCPR/C/PAK/CO/1, 23. August 2017, Rn. 35; Concluding observations: Estonia, CCPR/C/EST/CO/4, 18. April 2019, Rn. 29.
[883] EGMR, *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021, Rn. 497.
[884] Ebd., Rn. 498.

insbesondere auch vom Bestehen effektiver Aufsichtsmechanismen und Rechtsbehelfe für betroffene Individuen ab.[885] Gerade diese Erfordernisse, aber auch das Vorhandensein gesetzlicher Grundlagen, wurden in den letzten Jahren als kritische Punkte des *Intelligence Sharings* identifiziert.[886] Denn auch wenn in einem Staat die innerstaatlichen Systeme der Telekommunikationsüberwachung die menschenrechtlichen Anforderungen erfüllen, so erfolgen zwischenstaatliche Informationsaustausche häufig unreguliert und ohne effektive Beaufsichtigung.[887]

Im Rahmen der Interessenabwägung steht dem Individualinteresse auf Schutz der Privatsphäre auch hier das staatliche Sicherheitsinteresse gegenüber. Angesichts der heutigen Sicherheitsherausforderungen besteht ein besonderes Interesse der Staaten an dem zwischenstaatlichen Austausch von geheimdienstlich ausgespähten Telekommunikationsdaten. Denn angesichts der globalen Strukturen der heutigen Gefahren können Telekommunikationsdaten, die etwa außerhalb des eigenen Staatsgebiets fließen, durchaus für eine effektive Gefahrenprävention und -abwehr bedeutsam sein. Liegt die Gefahrenquelle nämlich außerhalb des eigenen Staatsgebiets, kann eine rein innerstaatliche Ermittlungspolitik tatsächlich im Zweifel unergiebig sein. Hierzu könnte der Staat einerseits theoretisch die Daten selbst durch extraterritoriale Überwachungsmaßnahmen ausspähen. Er kann aber auch aufgrund eines bilateralen oder multilateralen Vertrags über den Informationsaustausch die notwendigen Daten von einem anderen Staat erhalten. Freilich ist die zweite Alternative für den Staat mit weniger Aufwand verbunden, würde zudem in eiligen Situationen zu schnelleren Ergebnissen führen und würde ohne Verletzung der Staatssouveränität erfolgen. Für das Individuum ändert sich jedoch die – grundsätzlich hohe – Eingriffsintensität nicht. Dieser wichtige Punkt darf in der Interessenabwägung keinesfalls übersehen werden und muss gebührend gewichtet werden.

[885] Ebd., Rn. 499.

[886] Siehe dazu beispielsweise MRA Schweden UN Human Rights Committee, Concluding observations: Sweden, CCPR/C/SWE/CO/7, 28. April 2016, Rn. 37.

[887] Vgl. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Visit to Belgium, A/HRC/40/52/Add. 5, 27. Februar 2019, Rn. 61; Report of the United Nations High Commissioner for Human Rights, The Right to privacy in the digital age, A/HRC/39/29, 03. August 2018, Rn. 21. Siehe auch *Sepper,* Democracy, Human Rights, and Intelligence Sharing, S.169 ff.

Schlussbetrachtung und Ausblick

Die vorliegende Dissertation befasste sich mit der modernen geheimdienstlichen Telekommunikationsüberwachung und ihrer Vereinbarkeit mit dem im IPbpR und in der EMRK verankerten Menschenrecht auf Privatsphäre. Die Untersuchung hat gezeigt, dass diese internationalen Menschenrechtspakte trotz der rasanten technologischen Entwicklung einen weitreichenden Schutz vor geheimdienstlichen Überwachungsmaßnahmen gewähren.

Im 1. Abschnitt wurden die für die zentrale Fragestellung relevanten Grundlagen dargestellt. So konnte zunächst aufgezeigt werden, dass die moderne Informations- und Telekommunikationstechnologie längst Einzug in das private Leben eines Großteils der Weltbevölkerung gefunden hat. Das weite Schutzgut „Privatsphäre" umfasst heute infolgedessen auch eine digitale Dimension, die im alltäglichen Leben der Individuen schon lange keine Nebenrolle mehr spielt. Hinsichtlich der geheimdienstlichen Überwachung konnte anhand eines historischen Rückblicks dargelegt werden, dass sich die Überwachungsfunktion im Laufe der Geschichte nicht geändert hat, jedoch die Art der Risiken von der Antike bis heute einen deutlichen Wandel durchlaufen haben. In der heutigen Welt ist der internationale Terrorismus eine große sicherheitspolitische Herausforderung für die Staaten. Die Untersuchung hat an dieser Stelle gezeigt, dass Dezentralisierung und Unberechenbarkeit charakteristische Merkmale des heutigen Terrorismus sind, die die Bekämpfung dieses

Phänomens erheblich erschweren. Eine neuere Ausprägung des heutigen Terrorismus sind autonom agierende Individuen und kleine Terrorzellen, die aus der Mitte der Gesellschaft Terroranschläge ausüben. Diese Entwicklung hat die Gefahrenidentifizierung für die staatlichen Sicherheitsbehörden zusätzlich erschwert. Infolge des Wandels der Gefahren für die Sicherheit der Staaten haben sich die Methoden der geheimdienstlichen Informationsbeschaffung gleichermaßen geändert. Nach einem kurzen Überblick über unterschiedliche Überwachungsmittel wurde sodann der Untersuchungsfokus auf die Telekommunikationsüberwachung gerichtet. Hier wurde zunächst festgestellt, dass die breite Nutzung der modernen Kommunikationstechnologie den Geheimdiensten letztlich einen nahezu unerschöpflichen Informationspool bietet. Die drei heute hauptsächlich durchgeführten Formen der Telekommunikationsüberwachung wurden an dieser Stelle vorgestellt: Der direkte geheimdienstliche Zugriff auf Kommunikationsnetzwerke, die Erlangung von Daten mithilfe von *Service Providern* und die Verschaffung von geheimdienstlichen Direktzugriffen auf private Kommunikationsgeräte. Diese Methoden der Telekommunikationsüberwachung bildeten den Untersuchungsgegenstad der nachfolgenden Abschnitte.

Der 2. Abschnitt widmete sich der juristischen Untersuchung von geheimdienstlichen Maßnahmen zur Telekommunikationsüberwachung innerhalb der Staatsgrenzen. Das auf UN-Ebene und in der EMRK gewährleistete Menschenrecht auf Schutz der Privatsphäre ist dabei vorab dargestellt worden. Hier wurde jeweils zunächst herausgearbeitet, dass sowohl die UN-Richtlinien zum Datenschutz als auch die europäische Datenschutzkonvention wichtige Impulse für die Schaffung einer globalen Kultur des Datenschutzes setzen. Die europäische Datenschutzkonvention ist jedoch – insbesondere nach ihrer Modernisierung von 2018 – umfassender.

Das Augenmerk der Untersuchung richtete sich auf den Schutz der Korrespondenz und der personenbezogenen Daten gemäß Art. 17 IPbpR und Art. 8 EMRK, die für die zentrale Fragestellung der Dissertation relevant waren. Grundlage dieser Analysen war einerseits die verbindliche und umfassende Spruchpraxis des EGMR sowie die bedeutenden Stellungnahmen des UN-Menschenrechtsausschusses. Im Ergebnis wurde festgestellt, dass der MRA und der EGMR im Wege der dynamischen Auslegung auch moderne Telekommunikationsmittel unter „*correspondence*“ fassen und den Schutz der personenbezogenen Daten aus „*privacy*“ in Art. 17 IPbpR und aus „*private life*“ in Art. 8 EMRK ableiten. Ein weiteres wichtiges Ergebnis war, dass auch die Vertraulichkeit und die ungestörte Übertragung von Telekommunikationsverkehrsdaten (Metadaten) geschützt sind. Hier hat sich im Vergleich gezeigt, dass die Spruchpraxis des EGMR zur Auslegung von Art. 8 EMRK und speziell zum Schutz der Korrespondenz und der personenbezogenen Daten deutlich umfassender ist. Die Untersuchungen haben aber auch ergeben, dass der MRA im *General Comment* 16 wichtige Grundsätze des modernen Datenschutzes niedergelegt hat und diese im Laufe seiner Stellungnahmen in einer Reihe von *Concluding Observations* konkretisiert und weiterentwickelt hat. Angesichts dessen ist nach hier

vertretener Auffassung eine Neufassung des *General Comment* 16 von 1988 zwar nicht zwingend notwendig, sie würde allerdings eine begrüßenswerte Zusammenstellung der bisher entwickelten Judikatur des MRA im Bereich des Schutzes der personenbezogenen Daten unter Art. 17 IPbpR darstellen. Sie würde dem MRA auch die Gelegenheit geben, sich ausdrücklich zu einzelnen Fragen der Auslegung des Art. 17 IPbpR angesichts der modernen Informations- und Kommunikationstechnologie zu äußern.

Nach hier vertretener Auffassung und in Anlehnung an die Praxis des EGMR und des MRA ist in Fällen der Telekommunikationsüberwachung der Schutzbereich beider Ausprägungen der Privatsphäre – nämlich der Schutz der Korrespondenz und der Schutz der personenbezogenen Daten – nebeneinander eröffnet. So wurde auf dieser Grundlage festgestellt, dass die geheimdienstlichen Methoden zur Telekommunikationsüberwachung Eingriffe in die Integrität und Vertraulichkeit der Korrespondenz und der personenbezogenen Daten zugleich darstellen. Einer ausführlichen Betrachtung wurde zudem die Frage nach dem Vorliegen eines Eingriffs durch nationale Gesetze zur Telekommunikationsüberwachung unterzogen.

Im Rahmen der Überprüfung der Vereinbarkeit der Telekommunikationsüberwachung mit dem Menschenrecht auf Privatsphäre wurde zunächst ermittelt, dass die Schrankenregelungen in Art. 17 IPbpR und in Art. 8 EMRK gleiche Voraussetzungen für die Rechtfertigung von Eingriffen normieren. Hinsichtlich der einzelnen Voraussetzungen für die Bestimmtheit der Gesetze ist die Judikatur beider Spruchkörper sehr ähnlich. Zur Überprüfung der Menschenrechtskonformität von geheimdienstlichen Überwachungsmaßnahmen richten die Spruchkörper – insbesondere der EGMR in seiner umfassenden einschlägigen Jurisprudenz – ihr Augenmerk auf die Verhältnismäßigkeit, und zwar insbesondere auf die Angemessenheit. Dies spiegelte sich auch in der vorliegenden Untersuchung wider. Die Untersuchungen haben gezeigt, dass die Eingriffsintensität der Telekommunikationsüberwachung grundsätzlich hoch ist. Dabei kann der Intensitätsgrad einzelner Maßnahmen je nach Fallkonstellation variieren. In den einzelnen Fallkonstellationen wirken sich Faktoren wie Dauer und Erfassung sensibler Daten auf die Eingriffsintensität aus, wobei eine Kumulation mehrerer Faktoren zu einer erheblichen Intensivierung des Eingriffs führt. Die Angemessenheit der Maßnahmen hängt insbesondere auch davon ab, ob die zugrundeliegenden Gesetze eine unabhängige Genehmigung und Aufsicht regulieren. Hier gehen beide Spruchkörper vom Grundsatz der richterlichen Involvierung in der Genehmigung und Beaufsichtigung von Überwachungsmaßnahmen aus. Nach Ansicht des Gerichtshofs können auch nicht-juristische Organe diese Funktionen erfüllen, solange sie unabhängig agieren. Der MRA scheint neuerdings diesen Standpunkt gleichermaßen zu vertreten. Die Untersuchungen haben zudem offenbart, dass die Existenz effektiver Rechtsmittel für die Angemessenheit der Maßnahmen bedeutsam ist. In diesem Zusammenhang hat sich der MRA in jüngster Zeit ausdrücklich für eine *ex post* Benachrichtigung betroffener Individuen ausgesprochen. Der EGMR lässt wiederum als Ausnahme für eine

Benachrichtigung den Fall zu, dass eine effektive gerichtliche Überprüfung auch bei bloßem Überwachungsverdacht des Individuums möglich ist.

Der spezielle Fall der Massenüberwachungen wurde gesondert untersucht. Die Auswertung der Stellungnahmen des MRA hat dabei gezeigt, dass der Ausschuss eine kritische Haltung eingenommen hat und eine Rechtfertigung von Massenüberwachungsprogrammen nur unter strenger Berücksichtigung aller Kriterien des Art. 17 IPbpR zuzulassen scheint.

Die Entwicklungen der Jurisprudenz des EGMR zur Massenüberwachungen wurden sodann dargestellt. In der ersten Phase seiner Spruchpraxis beurteilte der Gerichtshof die Massenüberwachung nach den gleichen Maßstäben, die für die Einzelfallüberwachung entwickelt wurden. In den Entscheidungen *Centrum för rättvisa v. Sweden* und *Big Brother Watch and Others v. The United Kingdom* aus dem Jahr 2021 stellt er nunmehr einen modifizierten Kriterienkatalog auf. Dieser beurteilt Massenüberwachungen nicht strenger, allerdings sind die Kriterien an den spezifischen Eigenschaften der Massenüberwachung angepasst.

Die Untersuchungen im 2. Abschnitt haben im Ergebnis verdeutlicht, dass geheimdienstliche Maßnahmen zur Telekommunikationsüberwachung mit dem in Art. 17 IPbpR und Art. 8 EMRK niedergelegten Menschenrecht auf Privatsphäre kompatibel sein können. Sie haben aber auf der anderen Seite ebenso gezeigt, dass die Überwachung der Telekommunikation nicht grenzenlos geschehen darf. Eine technisch durchaus mögliche uferlose Ausspähung der Korrespondenzen und personenbezogenen Daten von Individuen stößt damit an rechtliche Grenzen, die sich aus den internationalen Menschenrechtsverpflichtungen der Staaten ergeben. Diesem Ergebnis steht auch nicht die Tatsache entgegen, dass der IPbpR und die EMRK zu einer Zeit in Kraft getreten sind, in der solche weitreichenden Formen der Telekommunikationsüberwachung weder durchgeführt, noch für möglich gehalten wurden. So sind die Menschenrechtspakte aufgrund der dynamischen Auslegung durch die Spruchorgane in der Lage, Schutz vor modernen Überwachungsmitteln zu bieten. Der MRA und der EGMR haben durch Auslegung klare Kriterien und Grenzen entwickelt, an denen die Menschenrechtskonformität von Überwachungsmaßnahmen zu beurteilen ist. Dabei hat die Auswertung der einschlägigen Spruchpraxis im Vergleich zueinander ergeben, dass die Judikatur des EGMR umfassender ist und auch über Detailfragen geurteilt wurde. Die einschlägigen Stellungnahmen des MRA sind hingegen in der Anzahl bislang überschaubar, jedoch sind zu allen wesentlichen Rechtsfragen in diesem Bereich Äußerungen des Ausschusses vorhanden. Die geheimdienstliche Überwachungspraxis der Staaten wird dem Ausschuss unzweifelhaft im Rahmen künftiger Staatenberichtsverfahren und möglicherweise auch eingehender Individualbeschwerden Anlass zur vertiefenden Stellungnahme geben, die er im Übrigen auch in einer Neufassung des *General Comment* 16 zusammenführen könnte.

Im 3. Abschnitt wurde das Phänomen der grenzüberschreitenden Telekommunikationsüberwachung untersucht.

Als Grundvoraussetzung einer Menschenrechtsverletzung durch die drittstaatliche Überwachung wurde zunächst die extraterritoriale Anwendbarkeit der Menschenrechtspakte geprüft. Nach hier vertretener Auffassung ist der Auslegung des MRA sowie des IGH und der allgemeinen Staatenpraxis zuzustimmen, wonach die Begriffe „*jurisdiction*“ und „*territory*“ in Art. 2 Abs. 1 IPbpR alternativ zueinander stehen. Demzufolge sind die Paktstaaten auch gegenüber Individuen außerhalb des Staatsgebiets zur Achtung und Gewährleistung der Paktgarantien verpflichtet, die sich unter ihrer Jurisdiktion befinden. Der EGMR legt dahingegen die Jurisdiktionsklausel in Art. 1 EMRK restriktiv aus. In der Entscheidung *Banković* legte er eine Regel-Ausnahme-Formel zugrunde, wonach grundsätzlich ein territorialer Jurisdiktionsbegriff gilt und eine extraterritoriale Anwendbarkeit der Konvention nur in Ausnahmefällen möglich sei. In seiner anschließenden kasuistischen Rechtsprechung erweiterte der Gerichtshof diesen Ausnahmekatalog um weitere Fälle und öffnete allmählich den Raum für eine extraterritoriale Anwendbarkeit der Konvention. Hier zeigte sich im Vergleich eine offenere Haltung des MRA hinsichtlich der extraterritorialen Anwendbarkeit des Paktes und auf der anderen Seite einen restriktiven Standpunkt des EGMR. Trotz dieser unterschiedlichen Grundhaltungen sind inzwischen die bislang von beiden Spruchkörpern anerkannten Anwendungsfälle der extraterritorialen Geltung der Menschenrechtspakte vergleichbar. So hat die Entscheidungsanalyse beider Spruchkörper ergeben, dass einerseits eine extraterritoriale Jurisdiktionsausübung aufgrund effektiver territorialer Kontrolle – etwa in Fällen der militärischen Besetzung – möglich ist. In diesen Fällen ist der extraterritorial agierende Staat vollumfänglich zur Umsetzung aller Bestimmungen und Verpflichtungen des Paktes verpflichtet. Zudem kann extraterritoriale Jurisdiktionsausübung nach Ansicht des MRA durch effektive Kontrolle über Individuen begründet werden. Der EGMR setzt hierfür effektive Gewalt und Kontrolle über Individuen in Ausnahmefällen voraus.

Sodann stellte sich die Frage, inwieweit in Fällen der grenzüberschreitenden Telekommunikationsüberwachung eine extraterritoriale Anwendbarkeit des IPbpR und der EMRK zu begründen ist. In der vorliegenden Dissertation konnte ein Konzept entwickelt werden, das die extraterritoriale Geltung der Menschenrechtspakte in Fällen grenzüberschreitender Überwachungen begründen kann. Demnach ist eine extraterritoriale Jurisdiktionsausübung nicht nur aufgrund der Kontrolle über Territorien und Individuen möglich, sondern kann auch aufgrund der Kontrolle über menschenrechtlich relevante Schutzobjekte begründet werden. Auch Telekommunikationsdaten, die unter den Schutz der Vertraulichkeit der Korrespondenz gemäß Art. 17 IPbpR und Art. 8 EMRK fallen, sind Schutzobjekte, über die virtuelle Kontrolle ausgeübt werden kann. Nach hier vertretender Ansicht ist auf Rechtsfolgenseite die Begrenzung der menschenrechtlichen Verpflichtung des Drittstaates auf das Maß seiner Kontrollausübung geboten. So wäre der Drittstaat demnach

gegenüber den betroffenen Individuen zur Umsetzung der Menschenrechte verpflichtet, die durch die extraterritorialen Überwachungsmaßnahmen tangiert werden.

Weiterhin war zu untersuchen, inwieweit der Aufenthaltsstaat des überwachten Individuums durch die extraterritoriale Überwachung Menschenrechtsverpflichtungen verletzt. Hierbei ging es in erster Linie um die Verletzung von Schutzpflichten. Dabei wurde im Ergebnis festgestellt, dass der Aufenthaltsstaat gegenüber dem Individuum schutzverpflichtet ist, wenn er trotz Kenntnis oder Kennen-Müssens der Überwachungsmaßnahmen angemessene Schutzmaßnahmen unterlässt. In der Praxis kommen insbesondere diplomatische Maßnahmen als Mindestschutz in Betracht.

Weiterhin wurde festgestellt, dass eine Verantwortlichkeit des Aufenthaltsstaates auch aufgrund von Beihilfe gem. Art. 16 des ILC-Entwurfs zur Staatenverantwortlichkeit bestehen könnte. Wenn der Aufenthaltsstaat durch bewusste Hilfshandlungen die drittstaatliche Überwachung der Individuen auf seinem Staatsgebiet unterstützt und damit als fördernder Faktor in dieser menschenrechtlichen Eingriffshandlung involviert ist, ist eine Beihilfe im Sinne dieser völkergewohnheitsrechtlichen Norm gegeben. Im Rahmen der rechtlichen Hinterleuchtung der heute gängigen Praxis des geheimdienstlichen Informationsaustausches hat sich gezeigt, dass die Staaten auch hierbei umfassend an ihre menschenrechtlichen Verpflichtungen aus Art. 17 IPbpR und Art. 8 EMRK gebunden sind. Sie können mithin nicht im Wege des *Intelligence Sharings* strengere Vorschriften im eigenen Staat umgehen, sondern müssen auch in Fällen des Datentransfers zwischen Geheimdiensten alle menschenrechtlichen Vorgaben einhalten.

Im 3. Abschnitt konnte letztlich aufgezeigt werden, dass eine Weiterentwicklung der bisherigen Jurisprudenz der Spruchkörper zur extraterritorialen Jurisdiktionsausübung nicht nur möglich, sondern auch geboten ist. Die bisherige Spruchpraxis des MRA und des EGMR im Bereich der extraterritorialen Jurisdiktionsausübung basiert auf einer kasuistischen Vorgehensweise. Die extraterritoriale Anwendbarkeit der Menschenrechtspakte in Fällen der grenzüberschreitenden Telekommunikationsüberwachung wurde von den Spruchkörpern bislang nicht ausdrücklich als neue Fallgruppe bestätigt, wobei aufgrund der grundsätzlich offenen Haltung des MRA und seiner bisherigen Positionierung in einschlägigen *Concluding Observations* davon auszugehen ist, dass dieser eine extraterritoriale Anwendbarkeit des IPbpR befürwortet. Die fehlende ausdrückliche Bestätigung als neue Fallgruppe bedeutet jedoch nicht, dass extraterritoriale Überwachungen keine menschenrechtliche Verantwortlichkeit der involvierten Staaten begründen. Denn anderenfalls würde dies zum willkürlichen Ergebnis führen, dass Staaten an ihre menschenrechtlichen Verpflichtungen nicht gebunden wären, wenn sie Individuen im Ausland überwachen. Der MRA und der EGMR haben in ihrer bisherigen Jurisprudenz bereits bewiesen, dass scheinbare menschenrechtliche Schutzlücken in den Pakten, die infolge technischer Entwicklungen seit dem Inkrafttreten zutage treten, im Wege der dynamischen Auslegung geschlossen werden können. Dies muss für den Fall der über Staatsgrenzen

hinausgehenden Überwachungstechnologien der modernen Geheimdienste ebenso gelten. Gerade für den internationalen Menschenrechtsschutz spielt diese Auslegungsdynamik und die stetige Anpassung an gesellschaftliche Modernisierungsprozesse eine herausragende Rolle. Denn als universelle, über Staatsgrenzen hinausgehende Schutzinstrumente bieten der IPbpR und die EMRK einen Schutzstandard, der unabhängig von der rechtlichen Entwicklungsgeschwindigkeit der einzelnen Staaten einen Mindestschutz für Individuen bietet.

Die vorliegende Untersuchung hat in diesem Sinne dargelegt, dass die extraterritoriale Jurisdiktionsausübung grundsätzlich auch aufgrund der effektiven Kontrolle über menschenrechtlich relevante Schutzobjekte begründet werden kann. Dieses Konzept baut auf die bisher entwickelten Kriterien für die extraterritoriale Anwendbarkeit von Menschenrechtspakten auf und schließt die scheinbare Schutzlücke in Fällen der grenzüberschreitenden Überwachung. Sie führt zu dem sachgerechten Ergebnis, dass extraterritoriale Jurisdiktionsausübung auch durch grenzüberschreitende Maßnahmen zur Telekommunikationsüberwachung begründet werden kann. Staaten, die durch extraterritoriale Maßnahmen virtuelle Kontrolle über Telekommunikationsdaten von Individuen ausspähen, sind demnach an ihre Pflichten aus Art. 17 IPbpR und Art. 8 EMRK gebunden.

Die vorliegende Dissertation hat damit einerseits aufgezeigt, wie die (grenzüberschreitende) Telekommunikationsüberwachung angesichts des internationalen – konkret in Art. 17 IPbpR und Art. 8 EMRK kodifizierten – Menschenrechts auf Privatsphäre zu beurteilen ist. Sie hat Antworten auf menschenrechtliche Fragen gegeben, die sich aus dem Phänomen der modernen Telekommunikationsüberwachung ergeben. Aber die Untersuchung berührt weitere offene Forschungsfragen, die sich im Zusammenhang des Untersuchungsthemas stellen, aber nicht Gegenstand der vorliegenden Untersuchung waren.

So stellt sich angesichts der geheimdienstlichen Inanspruchnahme von privaten *Service Providern* die Frage, inwieweit eine völkerrechtliche Verantwortung dieser kooperierenden Unternehmen begründet werden kann. Die Dissertation hat sich allein mit der Verantwortlichkeit der Staaten aufgrund des Handelns ihrer Geheimdienste befasst. Durchaus interessant ist indes auch die Frage nach der Verantwortlichkeit von Unternehmen wie *Google*, *Facebook*, etc.[888] Des Weiteren ist das Thema der (grenzüberschreitenden) Telekommunikationsüberwachung ebenso auf Ebene der EU in den vergangenen Jahren brisant diskutiert worden, und war bereits Gegenstand von Entscheidungen des EuGH.[889]

[888] Diese Thematik scheint auch zunehmend ins Visier der internationalen Menschenrechtsspruchkörper zu geraten, siehe dazu beispielsweise UN Human Rights Committee, Concluding observations: Italy, CCPR/C/ITA/CO/6, 1. Mai 2017, Rn. 37.

[889] Siehe insbesondere EuGH, *Maximillian Schrems v. Data Protection Commissioner*, Rs. C-362/14, 6. Oktober 2015.

Summary

The International Protection of Privacy from Intelligence Surveillance

Intelligence Surveillance of Individuals' Telecommunications in the Light of the ICCPR and the ECHR

This dissertation examines intelligence surveillance of private telecommunications and its compatibility with the international human right to privacy in Art. 17 ICCPR and in Art. 8 ECHR. First, an overview of the working methods of modern intelligence services as well as the different forms of today's telecommunications surveillance is given. In a second step, domestic telecommunications surveillance is examined from a human rights perspective. The study has shown that the ICCPR and the ECHR provide comprehensive protection against the most modern forms of surveillance including bulk interception and set clear limits for the justification of such measures. The relevant jurisprudence of the UN Human Rights Committee and the European Court of Human Rights on the requirements for the justification of telecommunication's surveillance as provided by Article 17 ICCPR and Art. 8 ECHR are examined. For justification, several criteria apply in terms of the foreseeability of the underlying surveillance laws. Moreover, telecommunication's interception should be subject to authorisation and supervision by an independent authority and an effective remedy should be available. Finally, the extent to which the surveilling state and the state of residence violate their human rights obligations in cases

of cross-border telecommunications surveillance is analyzed. The first question in this context is whether human rights treaties are applicable in this extraterritorial scenario. The jurisdiction clauses of the human rights treaties are decisive in this regard. The main issue is whether the established definition of „jurisdiction“ for purposes of article 2 (1) ICCPR and Art. 1 (1) ECHR are applicable to extraterritorial communications surveillance. The present study develops a new case group of extraterritorial jurisdiction. The author shows that the extraterritorial exercise of jurisdiction can in principle also be justified based on effective control over specific objects relevant to human rights. According to this approach, telecommunications data are objects relevant to individual's right to correspondence and data protection. States that exercise virtual control over individuals' telecommunications data through extraterritorial surveillance measures are thus bound by their obligations under Art. 17 ICCPR and Art. 8 ECHR. For the state of residence, the question of its positive obligations to protect individuals on its territory from foreign surveillance measures is examined.

Literaturverzeichnis

Akandji-Kombe, Jean-François: Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights, in: Council of Europe (Hrsg.), Human rights handbooks, No. 7, Strasbourg 2007.
[zitiert: *Akandji-Kombe,* Positive obligations under the European Convention on Human Rights]

Amerasinghe, Chittharanjan F.: Diplomatic Protection, Oxford 2008.
[zitiert: *Amerasinghe,* Diplomatic Protection]

Andres, Richard B.: National Security and U.S. Constitutional Rights. The Road to Snowden, in Kulesza, Joanna/Balleste, Roy (Hrsg.), Cybersecurity and Human Rights in the Age of Cyberveillance, London 2015, S. 147–166.
[zitiert: *Andres*, National Security and U.S. Constitutional Rights, in Kulesza/Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance]

Asche, Josephine: Die Margin of Appreciation. Entwurf einer Dogmatik monokausaler richterlicher Zurückhaltung für den europäischen Menschenrechtsschutz, Heidelberg 2018 (Beiträge zum ausländischen öffentlichen Recht und Völkerrecht, Band 267).
[zitiert: *Asche,* Die Margin of Appreciation]

Aust, Helmut: The UN Human Rights Due Diligence Policy. An Effective Mechanism against Complicity of Peacekeeping Forces?, Journal of Conflict Security Vol. 20, Issue1 (2015), S. 61–73.
[zitiert: *Aust,* The UN Human Rights Due Diligence Policy]

Ballaschk, Julia: In the Unseen Realm. Transnational Intelligence Sharing in the European Union – Challenges to Fundamental Rights and Democratic Legitimacy, Stanford Journal of International Law Vol. 51, No. 1 (2015), S. 19–51.
[zitiert: *Ballaschk,* In the Unseen Realm. Transnational Intelligence Sharing in the European Union]

Beck, Reinhart: Sachwörterbuch der Politik, Stuttgart 1986.
[zitiert: *Beck*, Sachwörterbuch der Politik]

Besson, Samantha: The Extraterritoriality of the European Convention on Human Rights. Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to, Leiden Journal of International Law Vol. 25, Issue 4 (2012), S. 857–884.
[zitiert: *Besson,* The Extraterritoriality of the European Convention on Human Rights]

Biehl, Simon: Die Europäische Menschenrechtskonvention in internationalen und nicht-internationalen bewaffneten Konflikten, Baden-Baden 2020.
[zitiert: *Biel*, Die Europäische Menschenrechtskonvention in internationalen und nicht-internationalen bewaffneten Konflikten]

Bignami, Francesca/Resta, Giorgio: Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti, Eyal/Nolte, Georg (Hrsg.), Community Interests Across International Law, Oxford 2018, S. 357–380.
[zitiert: *Bignami/Resta*, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, in Benvenisti/Nolte (Hrsg.), Community Interests Across International Law]

Blancke, Stephan: Geheimdienste und globalisierte Risiken, Berlin 2006.
[zitiert: *Blancke,* Geheimdienste und globalisierte Risiken]

Bossuyt, Marc: Guide to the „Travaux Préparatoires“ of the International Covenant on Civil and Political Rights, Dordrecht 1987.
[zitiert: *Bossuyt,* Guide to the „Travaux Préparatoires“]

Bowden, Caspar: Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger. Themenpapier, in: Europäisches Parlament (Hrsg.), September 2013.
[zitiert: *Bowden*, Die Überwachungsprogramme der USA und ihre Auswirkungen auf die Grundrechte der EU-Bürger]

Buergenthal, Thomas: The U.N. Human Rights Committee, in: von Bogdandy, Armin/ Wolfrum, Rüdiger (Hrsg.), Max Planck Yearbook of United Nations Law, Vol. 5 (2001), S. 341–398.
[zitiert: *Buergenthal,* The U.N. Human Rights Committee in von Bogdandy/Wolfrum (Hrsg.), Max Planck Yearbook of United Nations Law]

Buergenthal, Thomas: To Respect and to Ensure. State Obligations and Permissible Derogations, in: Henkin, Louis (Hrsg.), The International Bill of Rights, New York 1981, S. 72–91.
[zitiert: *Buergenthal,* To Respect and to Ensure, in Henkin (Hrsg.), The International Bill of Rights]

Buermeyer, Ulf: Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007 (Heft 4), S. 154–166.
[zitiert: *Buermeyer,* Die „Online-Durchsuchung“]

Bygrave, Lee A.: Data Privacy Law. An International Perspective, New York 2014.
[*Bygrave*, Data Privacy Law]

Clement, Andrew/Obar, Jonathan A.: Canadian Internet „Boomerang“ Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges, in: Geist, Michael (Hrsg.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era, Ottawa 2015, S. 13–44.
[zitiert: *Clement/Obar:* Canadian Internet „Boomerang“ Traffic and Mass NSA Surveillance, in Geist (Hrsg.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era]

Crawford, James: The International Law Commission’s Articles on State Responsibility: Introduction, Text and Commentaries, Cambridge 2002.
[zitiert: *Crawford,* The International Law Commission’s Articles on State Responsibility]

Da Costa, Karen: The Extraterritorial Application of Selected Human Rights Treaties, Leiden 2013.
[zitiert: *Da Costa*, The Extraterritorial Application of Selected Human Rights Treaties]

Daase, Christopher: Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel, in: Daase, Christopher/Feske, Susanne/Peters, Ingo (Hrsg.), Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden 2002, S. 9–36.
[zitiert: *Daase*, Internationale Risikopolitik, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik]

Daase, Christopher: Terrorismus. Der Wandel von einer reaktiven zu einer proaktiven Sicherheitspolitik der USA nach dem 11. September, in: Daase, Christopher/Feske, Susanne/Peters, Ingo (Hrsg.), Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen, Baden-Baden 2002, S. 113–142.
[zitiert: *Daase,* Terrorismus, in Daase/Feske/Peters (Hrsg.), Internationale Risikopolitik]

De Schutter, Olivier: Globalization and Jurisdiction. Lessons from the European Convention on Human Rights, Baltic Yearbook of International Law, Vol. 6 (2006), S. 185–247.
[zitiert: *De Schutter,* Globalization and Jurisdiction. Lessons from the European Convention on Human Rights]

Dearlove, Richard: National Security and Public Anxiety. Our Changing Perceptions, in: Johnson, Loch K. (Hrsg.), The Oxford Handbook of National Security Intelligence, New York 2010, S. 33–39.
[zitiert: *Dearlove,* National Security and Public Anxiety, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence]

Dennis, Michael J.: Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation, The American Journal of International Law Vol. 99, Issue 1 (2005), S. 119–141.
[zitiert: *Dennis,* Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation]

Diffie, Whitfield/Landau, Susan: Communications Surveillance. Privacy and Security at Risk, Communications of the ACM Vol. 52, No. 11 (2009), S. 42–47.
[zitiert: *Diffie/Landau,* Communications Surveillance. Privacy and Security at Risk]

Dominicé, Christian: Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State, in: Crawford, James/Pellet, Alain/Olleson, Simon (Hrsg.), The Law of International Responsibility, Oxford 2010, S. 281–289.
[zitiert: *Dominicé,* Attribution of Conduct to Multiple States and the Implication of a State in the Act of Another State, in Crawford/Pellet/Olleson (Hrsg.), The Law of International Responsibility]

Drechsler, Hanno: Gesellschaft und Staat. Lexikon der Politik, 10. Auflage, München 2003.
[zitiert: *Drechsler,* Gesellschaft und Staat. Lexikon der Politik]

Dröge, Cordula: Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, Berlin 2003.
[zitiert: *Dröge,* Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention]

Eßer, Martin/Kramer, Philipp/von Lewinski, Kai: DSGVO/BDSG. Datenschutz-Grundverordnung/Bundesdatenschutzgesetz und Nebengesetze, Kommentar, 6. Auflage, Köln 2018.
[zitiert: *Bearbeiter* in Eßer/Kramer/von Lewinski, DSGVO/BDSG Kommentar]

Ferris, John: Signals Intelligence in War and Power Politics, 1914–2010, in Johnson, Loch K. (Hrsg.): The Oxford Handbook of National Security Intelligence, New York 2010, S. 155–171.
[zitiert: *Ferris,* Signals Intelligence in War and Power Politics, in Johnson (Hrsg.), Oxford Handbook of National Security Intelligence]

Friedel, Andreas: Blackbox. Parlamentarisches Kontrollgremium des Bundestags. Defizite und Optimierungsstrategien bei der Kontrolle der Nachrichtendienste, Wiesbaden 2019.
[zitiert: *Friedel,* Blackbox. Parlamentarisches Kontrollgremium des Bundestags]

Frowein, Jochen Abraham/Peukert, Wolfgang: Europäische Menschenrechtskonvention, EMRK-Kommentar, 3. Auflage, Kehl am Rhein 2009.
[zitiert: *Bearbeiter* in Frowein/Peukert, EMRK-Kommentar]

Fuchs, Christian/Goetz, John: Die Zelle. Rechter Terror in Deutschland, Reinbek bei Hamburg 2012 [zitiert: *Fuchs/Goetz,* Die Zelle. Rechter Terror in Deutschland]

Georgieva, Ilina: The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR, Utrecht Journal of International and European Law Vol. 31, No. 80 (2015), S. 104–130.
[zitiert: *Georgieva,* The Right to Privacy under Fire]

Gill, Peter/Phythian, Mark: Intelligence in an Insecure World, Cambridge 2006.
[zitiert: *Gill/Phythian*, Intelligence in an Insecure World]

Grabenwarter, Christoph: European Convention on Human Rights, Commentary, München 2014.
[zitiert: *Grabenwarter,* European Convention on Human Rights]

Greer, Steven: Universalism and Relatvism in the Protection of Human Rights in Europe. Politics, Law and Culture, in Agha, Petr (Hrsg.), Human Rights between Law and Politics. The Margin of Appreciation in Post-National Contexts, Portland 2017, S. 17–34.
[zitiert: *Greer*, Universalism and Relatvism in the Protection of Human Rights in Europe, in Agha (Hrsg.), Human Rights between Law and Politics]

Hagmann, Jonas: (In-)Security and the Production of International Relations. The politics of securitization in Europe, New York 2015 (Routledge Critical Security Studies Series).
[zitiert: *Hagmann*, (In-)Security and the Production of International Relations]

Heil, Georg: The Berlin Attack and the „Abu Walaa" Islamic State Recruitment Network, CTC Sentinel, Volume 10 (2017), S. 1–11.
[zitiert: *Heil,* The Berlin Attack and the „Abu Walaa" Islamic State Recruitment Network]

Hermstrüwer, Yoan: Informationelle Selbstgefährdung. Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Tübingen 2016 (Grundlagen der Rechtswissenschaften 31).
[zitiert: *Hermstrüwer,* Informationelle Selbstgefährdung]

Hildebrandt, Mireille: Extraterritorial Jurisdiction to Enforce in Cyberspace. Bodin, Schmitt, Grotius in Cyberspace, University of Toronto Law Journal, Vol. 63, Issue 2 (2013), S. 196–224.
[zitiert: *Hildebrandt,* Extraterritorial Jurisdiction to Enforce in Cyberspace]

Hulnick, Arthur S.: The Dilemma of Open Sources Intelligence: Is Osint really Intelligence?, in Johnson, Loch K. (Hrsg.), The Oxford Handbook of National Security Intelligence, New York 2010, S. 229–241.
[zitiert: *Hulnick*, The Dilemma of Open Sources Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence]

Jacobsen, Colin/Maier-Katkin, Daniel: Breivik's Sanity. Terrorism, Mass Murder, and the Insanity Defense, Human Rights Quarterly, Vol. 37, No.1 (2015), S. 137–152.
[zitiert: *Jacobsen/Maier-Katkin,* Breivik's Sanity. Terrorism, Mass Murder, and the Insanity Defense]

Jakob, Bernd: Geheime Nachrichtendienste und Globalisierung. Der Faktor „Intelligence" zwischen staatenweltlicher Bedrohungsanalyse und weltgesellschaftlicher Risikoperzeption, Frankfurt am Main u.a. 1999 (Europäische Hochschulschriften, Reihe XXXI Politikwissenschaft, Bd. 380).
[zitiert: *Jakob,* Geheime Nachrichtendienste und Globalisierung]

Jankowska-Gilberg, Magdalena: Das Al-Skeini-Urteil des Europäischen Gerichtshofs für Menschenrechte – eine Abkehr von Banković?, Archiv des Völkerrechts, Bd. 50 (2012), S. 61–74.
[zitiert: *Jankowska-Gilberg*, Das Al-Skeini-Urteil des Europäischen Gerichtshofs für Menschenrechte]

Johann, Christian: Menschenrechte im internationalen bewaffneten Konflikt. Zur Anwendbarkeit der Europäischen Menschenrechtskonvention und des Internationalen Paktes über bürgerliche und politische Rechte auf Kriegshandlungen, Berlin 2012 (Menschenrechtszentrum der Universität Potsdam Band 35).
[zitiert: *Johann,* Menschenrechte im internationalen bewaffneten Konflikt]

Johnson, Loch K. (Hrsg.): The Oxford Handbook of National Security Intelligence, New York 2010.
[zitiert: *Johnson (Hrsg.),* The Oxford Handbook of National Security Intelligence]

Johnson, Loch K.: National Security Intelligence, in Johnson, Loch K. (Hrsg.), The Oxford Handbook of National Security Intelligence, New York 2010, S 3–32. [zitiert: *Johnson,* National Security Intelligence, in Johnson (Hrsg.), The Oxford Handbook of National Security Intelligence]

Joseph, Sarah/Castan, Melissa: The International Covenant on Civil and Political Rights. Cases, Materials, and Commentary, 3. Auflage, New York 2013. [zitiert: *Joseph/Castan,* The International Covenant on Civil and Political Rights]

Kälin, Walter/Künzli, Jörg: Universeller Menschenrechtsschutz. Der Schutz des Individuums auf globaler und regionaler Ebene, 4. Auflage, Basel 2019. [zitiert: *Kälin/Künzli,* Universeller Menschenrechtsschutz]

Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, 2. Auflage, Wiesbaden 2013. [zitiert: *Kappes,* Netzwerk- und Datensicherheit]

Keller, Christian Michael: Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit. Der Einsatz von IMSI-Catchern, Hamburg 2008. [zitiert: *Keller,* Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit]

Keller, Christoph/Braun, Frank/Hoppe, René: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, Stuttgart 2015. [zitiert: *Keller/Braun/Hoppe,* Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen]

King, Hugh: The Extraterritorial Human Rights Obligations of States, Human Rights Law Review Vol. 9, Issue 4 (2009), S. 521–556. [zitiert: *King,* The Extraterritorial Human Rights Obligations of States]

Kittichaisaree, Kriangsak: Public International Law of Cyberspace (Law, Governance and Technology Series, Vol. 32), Switzerland 2017. [zitiert: *Kittichaisaree*, Public International Law of Cyberspace]

Kleinlein, Thomas/Rabenschlag, David: Auslandsschutz und Staatsangehörigkeit, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Band 67 (2007), S. 1277–1337. [zitiert: *Kleinlein/Rabenschlag,* Auslandsschutz und Staatsangehörigkeit]

Knightley, Phillip: Die Geschichte der Spionage im 20. Jahrhundert. Aufbau und Organisation, Erfolge und Niederlagen der großen Geheimdienste, Berlin 1990. [zitiert: *Knightley,* Die Geschichte der Spionage im 20. Jahrhundert]

Knightley, Phillip: The Second Oldest Profession, The Spy as Bureaucrat, Patriot, Fantasist and Whore, London 1986. [zitiert: *Knightley,* The Second Oldest Profession]

Krieger, Wolfgang: Geschichte der Geheimdienste. Von den Pharaonen bis zur NSA, 3. Auflage, München 2014.
[zitiert: *Krieger,* Geschichte der Geheimdienste]

Landau, Susan: Surveillance or Security?, The Risks Posed by New Wiretapping Technologies, Cambridge Massachusetts 2010.
[*Landau,* Surveillance or Security?]

Lefebvre, Stéphane: The Difficulties and Dilemmas of International Intelligence Cooperation, International Journal of Intelligence and Counterintelligence Vol. 16, Issue 4 (2003), S. 527–542.
[zitiert: *Lefebvre*, The Difficulties and Dilemmas of International Intelligence Cooperation]

Loideain, Nora Ni: EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, Issue 2 (2015), S. 53–62.
[zitiert: *Loideain*, EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era]

Lowenthal, Mark M.: Intelligence, From Secrets to Policy, 6. Auflage, Los Angeles 2014.
[zitiert: *Lowenthal,* Intelligence. From Secrets to Policy]

Lyon, David: Surveillance after Snowden, Cambridge 2015.
[zitiert: *Lyon,* Surveillance after Snowden]

Margulies, Peter: The NSA in Global Perspective. Surveillance, Human Rights, and International Counterterrorism, Fordham Law Review Vol. 82, Issue 5 (2014), S. 2137–2167.
[zitiert: *Margulies,* The NSA in Global Perspective]

McGoldrick, Dominic: A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee, International & Comparative Law Quarterly Vol. 65, Issue 1 (2016), S. 21–60.
[zitiert: *McGoldrick,* A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee]

Meier, Ernst-Christoph/Hannemann, Andreas/Meyer zum Felde, Rainer: Wörterbuch zur Sicherheitspolitik - Deutschland in einem veränderten internationalen Umfeld, 8. Auflage, Hamburg 2012.
[zitiert *Meier/Hannemann/Meyer zum Felde,* Wörterbuch zur Sicherheitspolitik]

Milanovic, Marko: Al-Skeini and Al-Jedda in Strasbourg, The European Journal of International Law Vol. 23, Issue 1 (2012), S. 121–139.
[zitiert: *Milanovic,* Al-Skeini and Al-Jedda in Strasbourg]

Milanovic, Marko: Extraterritorial Application of Human Rights Treaties. Law, Principles and Policy, New York 2011.
[zitiert: *Milanovic,* Extraterritorial Application of Human Rights Treaties]

Milanovic, Marko: Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal Vol. 56, No. 1 (2015), S. 81–146.
[zitiert: *Milanovic*, Human Rights Treaties and Foreign Surveillance]

Moser-Knierim, Antonie: Vorratsdatenspeicherung. Zwischen Überwachungsstaat und Terrorabwehr, Wiesbaden 2014 (DuD-Fachbeiträge).
[zitiert: *Moser-Knierim,* Vorratsdatenspeicherung]

Mowbray, Alastair: Cases, Materials, and Commentary on the European Convention on Human Rights, 3. Auflage, Oxford 2012.
[zitiert: *Mowbray*, European Convention on Human Rights]

Moynihan, Harriet: Aiding and Assisting: The Mental Element under Article 16 of the International Law Commission's Articles on State Responsibility, International and Comparative Law Quarterly Vol. 67, Issue 2 (2018), S. 455–471.
[zitiert: *Moynihan*, Aiding and Assisting]

Müller, Andreas: Strategischer Nachrichtendienst und Informationsmanagement?. Neudefinition nachrichtendienstlicher Aufgaben in der Informationsgesellschaft, in Zoller, Manfred/Korte, Guido (Hrsg.), Nachrichtendienste in der Informationsgesellschaft. Zur Neubestimmung des nachrichtendienstlichen Aufgabenspektrums am Beispiel internationaler Terrorismus und Proliferation (Beiträge zur inneren Sicherheit Brühl, Band 12), Brühl 2000, S. 31–45.
[zitiert: *Müller*, Strategischer Nachrichtendienst und Informationsmanagement?, in Zoller/Korte (Hrsg.), Nachrichtendienste in der Informationsgesellschaft]

Murray, Daragh: Practitioners' Guide to Human Rights Law in Armed Conflict, London 2016.
[zitiert: *Murray,* Practitioners' Guide to Human Rights Law in Armed Conflict]

Nardell, Gordon: Levelling Up: Data Privacy and the European Court of Human Rights, in Gutwirth, Serge/Poullet, Yves/De Hert, Paul (Hrsg.), Data Protection in a Profiled World, Heidelberg/London/New York 2010, S. 43–52.
[zitiert: *Nardell,* Levelling Up: Data Privacy and the ECHR, in Gutwirth/Poullet/De Hert (Hrsg.), Data Protection in a Profiled World]

Ney, Peter/Smith, Ian/Cadamuro, Gabriel/Kohno, Tadayoshi: SeaGlass. Enabling City-Wide IMSI-Catcher Detection, Proceedings on Privacy Enhancing Technologies, Vol. 2017, No. 3, S 39–56.
[zitiert: *Ney/Smith/Cadamuro/Kohno*, SeaGlass. Enabling City-Wide IMSI-Catcher Detection]

Niebank, Jan-Christian: Menschenrechtliche Grenzen der zwischenstaatlichen Kooperation. Beihilfeverbote im Völkerrecht, in Deutsches Institut für Menschenrechte (Hrsg.), Beihilfe zu Menschenrechtsverstößen vermeiden – außenpolitische Zusammenarbeit kritisch prüfen (Analyse November 2017), Berlin 2017, S. 11–22.
[zitiert: *Niebank,* Menschenrechtliche Grenzen der zwischenstaatlichen Kooperation]

Nowak, Manfred: The Effectiveness of the International Covenant on Civil and Political Rights – Stocktaking after the first eleven Sessions of the UN-Human Rights Committee, Human Rights Law Journal Vol. 1, No. 1–4 (1980), S. 136–170.
[zitiert: *Nowak,* The Effectiveness of the International Covenant on Civil and Political Rights]

Nowak, Manfred: UN Covenant on Civil and Political Rights, CCPR Commentary, 2. Auflage, Kehl am Rhein 2005.
[zitiert: *Nowak*, CCPR Commentary]

Omand, David: The Cycle of Intelligence, in Dover, Robert/Goodman, Michael S./ Hillebrand, Claudia (Hrsg.), Routledge Companion to Intelligence Studies, Abingdon, New York 2014, S. 59–70.
[zitiert: *Omand,* The Cycle of Intelligence, in Dover/Goodman/Hillebrand (Hrsg.), Routledge Companion to Intelligence Studies]

Orakhelashvili, Alexander: Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights, European Journal of International Law Vol. 14, No. 3 (2003), S. 529–568.
[zitiert: *Orakhelashvili,* Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights]

Orwell, George: 1984, Übersetzt von Michael Walter, Ullstein Verlag, Berlin 2004.
[zitiert: *Orwell*, 1984]

Paefgen, Franziska: Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, Heidelberg 2016 (Beiträge zum ausländischen öffentlichen Recht und Völkerrecht, Band 259).
[zitiert: *Paefgen,* Persönlichkeitsrechte im Internet]

Papp, Andreas: Extraterritoriale Schutzpflichten. Völkerrechtlicher Menschenrechtsschutz und die deutsche Außenwirtschaftsförderung, Berlin 2013 (Schriften zum Völkerrecht, Band 203).
[zitiert: *Papp,* Extraterritoriale Schutzpflichten]

Peters, Anne: Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in Miller, Russel (Hrsg.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, Cambridge 2017, S. 145–179.
[zitiert: *Peters*, Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance, in Miller (Hrsg.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair]

PoKempner, Dinah: Cyberspace and State Obligations in the Area of Human Rights, in Ziolkowski, Katharina (Hrsg.), Peacetime regime for state activities in cyberspace: international law, international relations and diplomacy, Talinn 2013 (NATO CCD COE Publication), S. 239–258.
[zitiert: *PoKempner*, Cyberspace and State Obligations in the Area of Human Rights, in Zielkowski (Hrsg.), Peacetime regime for state activities in cyberspace]

Preissner-Polte, Anne: Wie der Blitz. Unternehmen, die Daten über Glasfasernetze transportieren, sind von den vielfältigen Möglichkeiten dieser modernen Übertragungssysteme begeistert. Kommunikation wird schnell wie das Licht, Warteschlangen vor den Rechenzentren lösen sich auf, manager magazin, Nr. 12 (1989), S. 262–269.
[zitiert: *Preissner-Polte:* Wie der Blitz]

Psychogiopoulou, Evangelia: The European Court of Human Rights, privacy and data protection in the digital era, in Brkan, Maja/Psychogiopoulou, Evangelia (Hrsg.), Courts, Privacy and Data Protection in the Digital Environment, Cheltenham 2017, S. 32–62.
[zitiert: *Psychogiopoulou*, The European Court of Human Rights, privacy and data protection in the digital era, in Brkan/Psychogiopoulou (Hrsg.), Courts, Privacy and Data Protection in the Digital Environment]

Ramakrishna, Kumar: From ‚Old' to ‚New' Terrorism. History, Current Trends and Future Prospects, in Gill, Martin (Hrsg.), The Handbook of Security, 2. Auflage, New York 2006, S. 159–181.
[zitiert: *Ramakrishna*, From ‚Old' to ‚New' Terrorism, in Gill (Hrsg.), Handbook of Security]

Ress, Georg: The Duty to Protect and to Ensure Human Rights under the European Convention on Human Rights, in Klein, Eckart (Hrsg.), The Duty to Protect and to Ensure Human Rights, Colloquium Potsdam, 1–3 July 1999, Berlin 2000, S. 165–205.
[zitiert: *Ress,* The Duty to Protect and to Ensure Human Rights under the European Convention on Human Rights, in Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights]

Roewer, Helmut/Schäfer, Stefan/Uhl, Matthias: Lexikon der Geheimdienste im 20. Jahrhundert, München 2003.
[zitiert: *Roewer/Schäfer/Uhl*, Lexikon der Geheimdienste im 20. Jahrhundert]

Rona, Gabor/Aarons, Lauren: State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace, Journal of National Security Law & Policy Vol. 8 (2016), S. 503–530.
[zitiert: *Rona/Aarons*: State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace]

Rooney, Jane M.: The Relationship between Jurisdiction and Attribution after *Jaloud v. Netherlands*, Netherlands International Law Review Vol. 62, Issue 3 (2015), S. 407–428.
[zitiert: *Rooney*, The Relationship between Jurisdiction and Attribution after Jaloud v. Netherlands]

Schabas, William A.: The European Convention on Human Rights, A Commentary, New York 2015.
[zitiert: *Schabas,* The European Convention on Human Rights]

Schaller, Christian: Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden, German Law Journal, Vol. 19, Issue 4 (2018), S. 941–980.
[zitiert: *Schaller*, Strategic Surveillance and Extraterritorial Basic Rights Protection]

Schiedermair, Stephanie: Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012.
[zitiert: *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht]

Schmidl, Michael: IT-Recht von A-Z – Accessprovider bis Zwischenspeicherung, 2. Auflage, München 2014.
[zitiert: *Schmidl,* IT-Recht von A-Z]

Schwelb, Egon: Civil and Political Rights: The International Measures of Implementation, The American Journal of International Law Vol. 62, Issue 4 (1968), S. 827–868.
[zitiert: *Schwelb,* Civil and Political Rights]

Seibert-Fohr, Anja: Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy, in David, Joseph E./Ronen, Yael/Shany, Yuval/Weiler, J.H.H. (Hrsg.), Strengthening Human Rights Protections in Geneva, Israel, the West Bank and Beyond, Cambridge 2021, S. 40–60.
[zitiert: *Seibert-Fohr,* Digital Surveillance, Meta Data and Foreign Intelligence Cooperation]

Sepper, Elizabeth: Democracy, Human Rights, and Intelligence Sharing, Texas International Law Journal Vol. 46, Issue 1 (2010), S. 151–207.
[zitiert: *Sepper,* Democracy, Human Rights, and Intelligence Sharing]

Shaack, Beth Van: The United States' Position on the Extraterritorial Application of Human Rights Obligations. Now is the Time for Change, International Law Studies Vol. 90 (2014), S. 20–65.
[zitiert: *Shaack,* The United States' Position on the Extraterritorial Application of Human Rights Obligations]

Shany, Yuval: Taking Universality Seriously: A Functional Approach to Extraterritoriality, International Human Rights Law, The Law & Ethics of Human Rights Vol. 7, Issue 1 (2013), S. 47–71.
[zitiert: *Shany,* Taking Universality Seriously]

Shulsky, Abram N./Schmitt, Gary A.: Silent Warfare. Understanding the World of Intelligence, 3. Auflage, Virginia 2002.
[zitiert: *Shulsky/Schmitt,* Silent Warfare]

Siemen, Birte: Datenschutz als europäisches Grundrecht, Berlin 2006 (Veröffentlichungen des Walther-Schücking-Instituts für Internationales Recht an der Universität Kiel, Band 158).
[zitiert: *Siemen,* Datenschutz als europäisches Grundrecht]

St. Vicent, Sarah: Preventing the Police State. International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector, in Cate, Fred H/Dempsey, James X. (Hrsg.), Bulk Collection. Systematic Government Access to Private-Sector Data, New York 2017, S. 355–380.
[zitiert: *St. Vincent,* Preventing the Police State, in Cate/Dempsey (Hrsg.), Bulk Collection]

Stahl, Sandra: Schutzpflichten im Völkerrecht – Ansatz einer Dogmatik, Heidelberg 2012 (Beiträge zum ausländischen öffentlichen Recht und Völkerrecht, Band 232).
[zitiert: *Stahl,* Schutzpflichten im Völkerrecht]

Stepanova, Ekaterina: Terrorism and Antiterrorism, in Kaldor, Mary/Rangelov, Iavor (Hrsg.), The Handbook of Global Security Policy (Handbook of Global Policy Series), Chichester 2014, S. 126–144.
[zitiert: *Stepanova,* Terrorism and Antiterrorism, in Kaldor/Rangelov (Hrsg.), The Handbook of Global Security Policy]

Störring, Lars Peter: Das Untermaßverbot in der Diskussion. Untersuchung einer umstrittenen Rechtsfigur, Berlin 2009.
[zitiert: *Störring,* Das Untermaßverbot in der Diskussion]

Stoyanova, Vladislava: Human Trafficking and Slavery Reconsidered. Conceptual Limits and States' Positive Obligations in European Law, Cambridge 2017.
[zitiert: Stoyanova, Human Trafficking and Slavery Reconsidered]

Szydlo, Marek: Extra-Territorial Application of the European Convention on Human Rights after Al-Skeini and Al-Jedda, International Criminal Law Review Vol. 12, No. 2 (2012), S. 271–291.
[zitiert: *Szydlo,* Extra-Territorial Application of the European Convention on Human Rights after Al-Skeini and Al-Jedda]

Taylor, Nick: To find the needle do you need the whole haystack? Global surveillance and principled regulation, The International Journal of Human Rights, Vol. 18, No. 1 (2014), S. 45–67.
[zitiert: *Taylor,* To find the needle do you need the whole haystack? Global surveillance and principled regulation]

Thallinger, Gerhard: Grundrechte und extraterritoriale Hoheitsakte. Auslandseinsätze des Bundesheeres und Europäische Menschenrechtskonvention, Wien 2008 (Europainstitut Wirtschaftsuniversität Wien Schriftenreihe, Band 29).
[zitiert: *Thallinger*, Grundrechte und extraterritoriale Hoheitsakte]

Tomuschat, Christian: Human Rights. Between Idealism and Realism, 3. Auflage, New York 2014 (The Collected Courses of the Academy of European Law, Band XIII/3).
[zitiert: *Tomuschat,* Human Rights. Between Idealism and Realism]

Unseld, Florian: Die Kommerzialisierung personenbezogener Daten, München 2010 (Rechtswissenschaftliche Forschung und Entwicklung, Band 769).
[zitiert: *Unseld,* Die Kommerzialisierung personenbezogener Daten]

Von Arnauld, Andreas: Souveränität als fundamentales Konzept des Völkerrechts, Die Friedens-Warte Vol. 89, No. 3/4 (2014), S. 51–72.
[zitiert: *Von Arnauld*, Souveränität als fundamentales Konzept des Völkerrechts]

Von Bernstorff, Jochen: Kerngehaltsschutz durch den UN-Menschenrechtsausschuss und den EGMR. Vom Wert kategorialer Argumentationsformen, Der Staat Vol. 50, No. 2 (2011), S. 165–190.
[zitiert: *Von Bernstrorff,* Kerngehaltsschutz durch den UN-Menschenrechtsausschuss und den EGMR]

Watt, Eliza: The right to privacy and the future of mass surveillance, The International Journal of Human Rights, Vol. 21, No. 7 (2017), S. 773–799.
[zitiert: *Watt,* The right to privacy and the future of mass surveillance]

Weber, Rolf H./Staiger, Dominic N.: Privacy versus Security. Identifying the Challenges in a Global Information Society, in Kulesza, Joanna/Balleste, Roy (Hrsg.), Cybersecurity and Human Rights in the Age of Cyberveillance, London 2015, S. 63–83.
[zitiert: *Weber/Staiger*, Privacy versus Security, in Kulesza/Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance]

Weidner-Braun, Ruth: Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichen Recht, Berlin 2012.
[zitiert: *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung]

Wilde, Ralph: Human Rights beyond Borders at the World Court. The Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties, Chinese Journal of International Law Vol. 12, Issue 4 (2013), S. 639–677.
[zitiert: *Wilde,* Human Rights beyond Borders at the World Court]

Wilde, Ralph: Triggering State Obligations Extraterritorially. The spatial test in certain Human Rights Treaties, Israel Law Review Vol. 40, Issue 2 (2007), S. 503–526.
[zitiert: *Wilde:* State Obligations Extraterritorially]

Wirtz, Sebastian/Harding, Ulf: Terroranschläge weltweit und in Europa. Historie, Überblick, aktuelle Lage, Notfall+ Rettungsmedizin Vol. 21, Issue 7 (2018), S. 553–559.
[zitiert: *Wirtz/Harding,* Terroranschläge weltweit und in Europa]

Wolff, Heinrich Amadeus/Brink, Stephan: Datenschutzrecht in Bund und Ländern – Grundlagen. Bereichsspezifischer Datenschutz. BDSG. Kommentar, München 2013.
[zitiert Bearbeiter in Wolff/Brink, Datenschutzrecht in Bund und Ländern, Kommentar]

Zech, Herbert: Information als Schutzgegenstand, Tübingen 2012 (Jus Privatum, Band 166).
[zitiert: *Zech,* Information als Schutzgegenstand]

Entscheidungsverzeichnis

MRA[890]

1. *Angel Estrella v. Uruguay,* No. 74/1980, CCPR/C/18/D/74/1980, 29. März 1983
2. *Annakkarage Suranjini Sadamali Pathmini Peiris v. Sri Lanka*, No. 1862/2009, CCPR/C/103/D/1862/2009, 18. April 2012
3. *Antonius Cornelis Van Hulst v. The Netherlands*, No. 903/1999, CCPR/C/82/D/903/1999, 15. November 2004
4. *Aumeeruddy-Cziffra et al v. Mauritius*, No. 35/1978, CCPR/C/12/D/35/1978, 09. April 1994
5. *Boodoo v. Trinidad and Tobago*, No. 721/1996, CCPR/C/74/D/721/1996, 02. April 2002

[890] Die Entscheidungen des MRA sind unter https://juris.ohchr.org/ abrufbar [zuletzt abgerufen 02.12.2021].

6. *Bordes and Temeharo v. France,* No. 645/1995, CCPR/C/57/D/645/1995, 22. Juli 1996
7. *Carlos Varela Nunez v. Uruguay,* No. 108/1981, CCPR/C/19/D/108/1981, 22. Juli 1983
8. *Coeriel and Aurik v. The Netherlands,* No. 453/1991, CCPR/C/52/D/453/1991, 9. Dezember 1994
9. *Crafton Tomlin v. Jamaica,* No. 589/1994, CCPR/C/57/D/589/1994, 16. Juli 1996
10. *Daniel Pinto v. Trinidad and Tobago,* No. 512/1992, CCPR/C/57/D/512/1992, 24. Juni 1994
11. *Keun-Tae Kim v. Republic of Korea,* No. 574/1994, CCPR/C/64/D/574/1994, 3. November 1998
12. *Larry James Pinkney v. Canada,* No. 27/1978, CCPR/C/OP/1 **at 95 (1985),** 29. Oktober 1981
13. *Leonid Raihman v. Latvia*, No. 1621/2007, CCPR/C/100/D/1621/2007, 30. November 2010
14. *Lilian Celiberti de Casariego v. Uruguay*, No. 56/1979, CCPR/C/13/D/56/1979, 29. Juli 1981
15. *Mabel Pereira Montero v. Uruguay,* No. 106/1981, CCPR/C/18/D/106/1981, 31. März 1983
16. *Miguel Angel Estrella v. Uruguay*, No. 74/1980, U.N. Doc. Supp. No. 40 (A/38/40), 29. März 1983
17. *Omar Sharif Baban v. Australia*, No. 1014/2001, CCPR/C/78/D/1014/2001, 6. August 2003
18. *S. S. v. Norway,* No. 79/1980, CCPR/C/15/D/79/1980, 2. April 1982
19. *Samuel Lichtensztejn v. Uruguay,* No. 77/1980, CCPR/C/18/D/77/1980, 31. März 1983
20. *Sergio Ruben Lopez Burgos v. Uruguay,* No. 52/1979, CCPR/C/13/D/52/1979, 29. Juli 1981

21. *Simunek v. Czech Republic,* No. 516/1992, CCPR/C/54/D/516/199, 19. Juli 1995
22. *Sophie Vidal Martins v. Uruguay,* No. 057/1979, CCPR/C/15/D/57/1979, 23. März 1982
23. *Toonen v. Australia*, No. 488/1992, CCPR/C/50/D/488/1992, 31. März 1994
24. *Vjatseslav Borzov v. Estonia,* No. 1136/2002, CCPR/C/81/D/1136/2002, 25. August 2004
25. *William Eduardo Delgado Páez v. Colombia*, No. 195/1985, CCPR/C/39/D/195/1985, 12. Juli 1990

EGMR[891]

1. *10 Human Rights Organisations and Others v. the United Kingdom* [Communicated Case], Rs. 24960/15, 24. November 2015
2. *Airey v. Ireland,* Rs. 6289/73, 09. Oktober 1979, Serie A 32
3. *Al-Saadoon and Mufdhi v. the United Kingdom*, Rs. 61498/08, 30. Juni 2009
4. *Al-Skeini and Others v. The United Kingdom* [GC], Rs. 55721/07, 7. Juli 2011, Rep. 2011
5. *Amann v. Switzerland* [GC], Rs. 27798/95, 16. Februar 2000, Rep. 2000-II
6. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Rs. 62540/00, 28. Juni 2007
7. *Banković and Others v. Belgium and Others* [GC], Rs. 52207/99, 12. Dezember 2001, Rep. 2001-XII
8. *Behrami and Behrami v. France and Saramati v. France, Germany and Norway* [GC], Rs. 71412/01, 78166/01, 2. Mai 2007

[891] Die Entscheidungen des EGMR und der EKMR sind auf der HUDOC-Datenbank des Europarates (abrufbar unter http://www.echr.coe.int/ECHR/EN/hudoc [zuletzt abgerufen 02.12.2021]) in den amtlichen Sprachfassungen abrufbar.

9. *Bernh Larsen Holding A S and Others v. Norway,* Rs. 24117/08, 14. März 2013
10. *Big Brother Watch and Others v. The United Kingdom* [GC], Rs. 58170/13, 62322/14 und 24960/15, 25. Mai 2021
11. *Botta v. Italy,* Rs. 21439/93, 24. Februar 1998, Rep. 1998-I
12. *Boyle and Rice v. The United Kingdom,* Rs. 9659/82, 9658/82, 27. April 1988, Serie A 131
13. *Budayeva and Others v Russia,* Rs. 15339/02, 11673/02, 15343/02, 20058/02, 21166/02, 20. März 2008, Rep. 2008
14. *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* [Communicated Case], Rs. 62322/14, 5. Januar 2015
15. *Campbell and Fell v. The United Kingdom,* Rs. 7819/77, 7878/77, 28. Juni 1984, Serie A 80
16. *Catan and Others v. Moldova and Russia* [GC], Rs. 43370/04, 18454/06, 8252/05, 19. Oktober 2012, Rep. 2012
17. *Cemalettin Canli v. Turkey,* Rs. 22427/04, 18. November 2008
18. *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], Rs. 47848/08, 17. Juli 2014, Rep. 2014
19. *Centrum för rättvisa v. Sweden* [GC], Rs. 35252/08, 25. Mai 2021
20. *Chappell v. The United Kingdom,* Rs. 10461/83, 30. März 1989, Serie A152-A
21. *Chauvy and Others v. France,* Rs. 64915/01, 29. Juni 2004, Rep. 2004-VI
22. *Copland v. The United Kingdom*, Rs. 62617/00, 03. April 2007, Rep. 2007-I
23. *Cyprus v. Turkey* [GC], Rs. 25781/94, 10. Mai 2001, Rep. 2001-IV
24. *De Wilde, Ooms and Versyp v. Belgium,* Rs. 2832/66, 2835/66, 2899/66, 18. November 1970, Serie A 12
25. *Dragojević v. Croatia,* Rs. 68955/11, 15. Januar 2015
26. *Drozd and Janousek v. France and Spain,* Rs. 12747/87, 26. Juni 1992, Serie A 240
27. *Dudgeon v, The United Kingdom,* Rs. 7525/76, 22. Oktober 1981, Serie A45

28. *El-Masri v. The former Yugoslav Republic of Macedonia*, Rs. 39630/09, 13.12.2012, Rep. 2012
29. *Fadeyeva v. Russia,* Rs. 55723/00, 09. Juni 2005, Rep. 2005-IV
30. *Golder v. The United Kingdom*, Rs. 4451/70, 21. Februar 1975, Serie A 18
31. *Halford v. The United Kingdom,* Rs. 20605/92, 25. Juni 1997, Rep. 1997-III
32. *Hämäläinen v. Finland* [GC], Rs. 37359/09, 16. Juli 2014, Rep. 2014
33. *Handyside v. The United Kingdom,* Rs. 5493/72, 07. Dezember 1976, Serie A 24
34. *Hassan v. The United Kingdom* [GC], Rs. 29750/09, 16. September 2014, Rep. 2014
35. *Hirsi Jamaa and Others v. Italy* [GC], Rs. 27765/09, 23. February 2012, Rep. 2012
36. *I. v. Finland,* Rs. 20511/03, 17. Juli 2008
37. *Ilaşcu and Others v. Moldova and Russia* [GC]*,* Rs. 48787/99, 8. Juli 2004, Rep. 2004-VII
38. *Iliya Stefanov v. Bulgaria,* Rs. 65755/01, 22. Mai 2008
39. *Iordachi and Others v. Moldova,* Rs. 25198/02, 10. Februar 2009
40. *Isaak v. Turkey,* Rs. 44587/98, 24. Juni 2008,
41. *Issa and Others v. Turkey,* Rs. 31821/96, 16. November 2004
42. *Jaloud v. The Netherlands* [GC], Rs. 47708/08, 20. November 2014, Rep. 2014
43. *Johnston and Others v. Ireland,* Rs. 9697/82, 18. Dezember 1986, Serie A 112
44. *Kallis and Androulla Panayi v. Turkey,* Rs. 45388/99, 27. Oktober 2009
45. *Keegan v. Ireland,* Rs. 16969/90, 26. Mai 1994, Serie A 290
46. *Kennedy v. The United Kingdom,* Rs. 26839/05, 18. Mai 2010
47. *Khmel v. Russia,* Rs. 20383/04, 12. Dezember 2013
48. *Klass and Others v. Germany*, Rs. 5029/71, 6. September 1978, Serie A 28

49. *Kopp v. Switzerland,* Rs. 23224/94, 25. März 1998, Rep. 1998-II
50. *Kruslin v. France,* Rs. 11801/85, 24. April 1990, Serie A 176-A
51. *Leander v. Sweden,* Rs. 9248/81, 26. März 1987, Series A116
52. *Liberty and Others v. The United Kingdom*, Rs. 58243/00, 01. Juli 2008
53. *Loizidou v. Turkey [GC],* Rs. 15318/89 (Merits), 18. Dezember 1996, Rep. 1996-VI
54. *Loizidou v. Turkey [GC],* Rs. 15318/89 (Preliminary Objections), 23. März 1995, Serie A 310
55. *López Ostra v. Spain,* Rs. 16798/90, 09. Dezember 1994, Serie A 303-C
56. *M.M. v. The United Kingdom,* Rs. 24029/07, 13. November 2012
57. *Malone v. The United Kingdom,* Rs. 8691/79, 26. April 1985, Serie A 95
58. *Marckx v. Belgium*, Rs. 6833/74, 13. Juni 1979, Serie A31
59. *McCann and Others v. Vereinigtes Königreich,* Rs. 18984/91, 27. September 1995, Serie A 324
60. *Medvedyev and Others v. France,* Rs. 3394/03, 29. März 2010, Rep. 2010
61. *Michaud v. France,* Rs. 12323/11, 6. Dezember 2012
62. *Mozer v. the Republic of Moldova and Russia* [GC]*,* Rs. 11138/10, 23. Februar 2016, Rep. 2016
63. *Niemitz v. Germany,* Rs. 13710/88, 16. Dezember 1992, Serie A251-B
64. *Öcalan v. Turkey* [GC], Rs. 46221/99, 12. Mai 2005, Rep. 2005-IV
65. *Öneryildiz v. Turkey* [GC], Rs. 48939/99, 30. November 2004, Rep. 2004-XII
66. *Osman v. The United Kingdom* [GC], Rs. 23452/94, 28. Oktober 1998, Rep. 1998-VIII
67. *P. and S. v. Poland*, Rs. 57375/08, 30. Oktober 2012
68. *P.G. and J.H. v. The United Kingdom,* Rs. 44787/98, 25. September 2001, Rep. 2001-IX
69. *Pad and Others v. Turkey,* Rs. 60167/00, 28. Juni 2007

70. *Peck v. The United Kingdom,* Rs. 44647/98, 28. January 2003, Rep. 2003-I
71. *Peev v. Bulgaria,* Rs. 64209/01, 26. Juli 2007
72. *Perry v. The United Kingdom,* Rs. 63737/00, 17. Juli 2003, Rep. 2003-IX
73. *Plattform „Ärzte für das Leben“ v. Austria,* Rs. 10126/82, 21. Juni 1988, Serie A139
74. *Pretty v. The United Kingdom,* Rs. 2346/02, 29. April 2002, Rep. 2002-III
75. *R.E. v. The United Kingdom,* Rs 62498/11, 27. Oktober 2015
76. *Rees v. The United Kingdom,* Rs. 9532/81, 17. Oktober 1986, Serie A 106
77. *Roman Zakharov v. Russia* [GC], Rs. 47143/06, 4. Dezember 2015
78. *Rotaru v. Romania* [GC],Rs. 28341/95, 4. Mai 2000, Rep. 2000-V
79. *S. and Marper v. The United Kingdom* [GC], Rs. 30562/04, 30566/04, 4. Dezember 2008
80. *Salakhov and Islyamova v. Ukraine,* Rs. 28005/08, 14. März 2013
81. *Salomou and Others v. Turkey,* Rs. 36832/97, 24. Juni 2008
82. *Sandu and Others v. the Republic of Moldova and Russia*, Rs. 21034/05, 41569/04, 41573/04, 41574/04, 7105/06, 9713/06, 18327/06 und 38649/06, 17. Juli 2018,
83. *Segerstedt-Wiberg and Others v. Sweden,* Rs. 62332/00, 6. Juni 2006, Rep. 2006-VII
84. *Silver and Others v. The United Kingdom*, Rs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, 25. März 1983, Serie A 61
85. *Szabó and Vissy v. Hungary*, Rs. 37138/14, 12. Januar 2016
86. *Uzun v Germany,* Rs. 35623/05, 2. September 2010
87. *Valenzuela Contreras v. Spain*, Rs. 27671/95, 30. Juli 1998, Rep. 1998-V
88. *Von Hannover v. Germany,* Rs. 59320/00, 24. Juni 2004, Rep. 2004-VI
89. *Weber and Saravia v. Germany,* Rs. 54934/00, 29. Juni 2006, Rep. 2006-XI

90. *Wieser and Bicos Beteiligungen GmbH v. Austria*, Rs. 74336/01, 16. Oktober 2007, Rep. 2007-IV
91. *X and Y v. the Netherlands*, Rs. 8978/80, 26. März 1985, Serie A 91
92. *Y.F. v. Turkey,* Rs. 24209/94, 22. Juli 2003, Rep. 2003-IX
93. *Young, James and Webster v. The United Kingdom,* Rs. 7601/76 7806/77, 13. August 1981, Serie A 44
94. *Z. v. Finland*, Rs. 22009/93, 25. Februar 1997, Rep. 1997-I

EKMR

1. *Cyprus v. Turkey*, Rs. 6780/74 und 6950/75, 26. Mai 1975, D.R.2, S. 125
2. *Cyprus v. Turkey*, Rs. 8007/77, 10. Juli 1978, D.R.13, S. 85
3. *Dobberstein v. Germany,* Rs. 25045/94, 12. April 1994
4. *Hess v. the United Kingdom*, Rs. 6231/73, 28. Mai 1975, D.R. 2, S. 72
5. *Jüngling and Others v. Germany,* Rs. 22353/93, 18. Oktober 1995
6. *Luck v. Germany,* Rs. 24928/94, 30. November 1994
7. *Nadler and Reckziegel v. Germany*, Rs. 27718/95, 12. April 1996
8. *Tugar v. Italy,* Rs. 22869/93, 18. Oktober 1995, D.R.83-A, S. 26
9. *W. v. the United Kingdom*, Rs. 9348/81, 28. Februar 1983, D.R. 32, S. 190
10. *X and Y v. Switzerland,* Rs. 7289/75 und 7349/76, 14. Juli 1977, D.R. 9, S. 57
11. *X. v. the Federal Republic of Germany,* Rs. 1611/62, 25. September 1965, Yearbook 8, S. 158
12. *X. v. the United Kingdom*, Rs. 7547/76, 15. Dezember 1977, D.R. 12, S. 73

EUGH

1. *Digital Rights Ireland Ltd v. Minister for Communications & Others*, Rs. C-293/12 und C-594/12, 8. April 2014
2. *Maximillian Schrems v. Data Protection Commissioner*, Rs. C-362/14, 6. Oktober 2015

IGH

1. Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo), Merits, Judgment, I.C.J. Reports 2010, S. 639
2. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment (2007) I.C.J Reports 2007, S. 150
3. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, 19. Dezember 2005, I.C.J. Reports 2005, S.168
4. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9. Juli 2004, I.C.J. Reports 2004, S.136

BVerfG

1. BVerfGE 65, 1, Urteil vom 15. Dezember 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 (Volkszählung)
2. BVerfGE 125, 260, Urteil vom 02. März 2010 – 1 BvR 256/08 (Vorratsdatenspeicherung)



Die Dissertation untersucht die geheimdienstliche Überwachung privater Telekommunikation und ihre Vereinbarkeit mit dem internationalen Menschenrecht auf Privatsphäre in Art. 17 ICCPR und in Art. 8 EMRK. Diese Artikel bieten einen umfassenden Schutz gegen die modernsten Formen der Überwachung, einschließlich der Massenüberwachung. Es gelten konkrete Kriterien für die Bestimmtheit der Überwachungsgesetze. Die Überwachung muss zudem durch unabhängige Behörden genehmigt sowie kontrolliert werden und effektive Rechtsmittel müssen zur Verfügung stehen. Darüber hinaus wird in der Studie untersucht, inwieweit der überwachende Staat und der Aufenthaltsstaat bei grenzüberschreitender Überwachung ihre menschenrechtlichen Verpflichtungen verletzen. Die zentrale Frage ist, ob die bisherigen Definitionen der „jurisdiction" auf dieses extraterritoriale Szenario anwendbar sind. Die extraterritoriale Ausübung der Jurisdiktion kann sich auch auf die Kontrolle über bestimmte menschenrechtlich relevante Objekte stützen. Diesem Ansatz zufolge sind Telekommunikationsdaten Objekte, die für das Recht des Einzelnen auf Korrespondenz und Datenschutz relevant sind.

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

ISBN: 978-3-86395-547-2

Universitätsverlag Göttingen